2011

Cognitive Security Framework For Heterogeneous Sensor Network Using Swarm Intelligence

Rajani Muraleedharan
Syracuse University

Abstract

Rapid development of sensor technology has led to applications ranging from academic to military in a short time span. These tiny sensors are deployed in environments where security for data or hardware cannot be guaranteed. Due to resource constraints, traditional security schemes cannot be directly applied. Unfortunately, due to minimal or no communication security schemes, the data, link and the sensor node can be easily tampered by intruder attacks.

This dissertation presents a security framework applied to a sensor network that can be managed by a cohesive sensor manager. A simple framework that can support security based on situation assessment is best suited for chaotic and harsh environments. The objective of this research is designing an evolutionary algorithm with controllable parameters to solve existing and new security threats in a heterogeneous communication network. An in-depth analysis of the different threats and the security measures applied considering the resource constrained network is explored. Any framework works best, if the correlated or orthogonal performance parameters are carefully considered based on system goals and functions. Hence, a trade-off between the different performance parameters based on weights from partially ordered sets is applied to satisfy application specific requirements and security measures.

The proposed novel framework controls heterogeneous sensor network requirements, and balance the resources optimally and efficiently while communicating securely using a multi-objection function. In addition, the framework can measure the affect of single or combined denial of service attacks and also predict new attacks under both cooperative and non-cooperative sensor nodes. The cognitive intuition of the framework is evaluated under different simulated real time scenarios such as Health-care monitoring, Emergency Responder, VANET, Biometric security access system, and Battlefield monitoring.

The proposed three-tiered Cognitive Security Framework is capable of performing situation assessment and performs the appropriate security measures to maintain reliability and security of the system. The first tier of the proposed framework, a cross-layer cognitive security protocol defends the communication link between nodes during denial-of-Service attacks by re-routing data through secure nodes. The cognitive nature of the protocol balances resources and security making optimal decisions to obtain reachable and reliable solutions. The versatility and robustness of the protocol is justified by the results obtained in simulating health-care and emergency responder applications under Sybil and Wormhole attacks. The protocol considers metrics from each layer of the network model to obtain an optimal and feasible resource efficient solution.

In the second tier, the emergent behavior of the protocol is further extended to mine information from the nodes to defend the network against denial-of-service attack using Bayesian models. The jammer attack is considered the most vulnerable attack, and therefore simulated vehicular ad-hoc network is experimented with varied types of jammer. Classification of the jammer under various attack scenarios is formulated to predict the genuineness of the attacks on the sensor nodes using receiver operating characteristics. In addition to detecting the jammer attack, a simple technique of locating the jammer under cooperative nodes is implemented. This feature enables the network in isolating the jammer or the reputation of node is affected, thus removing the malicious node from participating in future routes.

Finally, a intrusion detection system using ‘bait’ architecture is analyzed where resources is traded-off for the sake of security due to sensitivity of the application. The architecture strategically enables ant agents to detect and track the intruders threatening the network. The proposed framework is evaluated based on accuracy and speed of intrusion detection before the network is compromised. This process of detecting the intrusion earlier helps learn future attacks, but also serves as a defense countermeasure. The simulated scenarios of this dissertation show that Cognitive Security Framework is best suited for both homogeneous and heterogeneous sensor networks.

COGNITIVE SECURITY FRAMEWORK FOR HETEROGENEOUS SENSOR NETWORK USING SWARM INTELLIGENCE

By

Rajani Muraleedharan Sreekumaridevi

B.E. University of Madras, India

M.S. Syracuse University, Syracuse, NY

DISSERTATION

Submitted in partial fulfillment of the requirements for the degree
of Doctor of Philosophy in Electrical Engineering in the Graduate
School of Syracuse University

August 2011

Table of Contents

List of Figures

List of Tables

This research work is dedicated to
my family, advisors, faculty, colleagues and friends who have
supported me throughout this journey.

Acknowledgment

"Clouds come floating into my life, no longer to carry rain or usher storm, but to add color to my sunset sky." - Rabindranath Tagore

My time at Syracuse University was a joyful and colorful journey with some winding roads but several individuals guided me to achieve my goal. Just as the clouds in Tagore's quote these individuals shaped and lifted my spirit, kindled my desire to fulfill my dreams and supported me through this journey. To these individuals, I wish to say "THANK YOU".

I wish to express my heartfelt gratitude and thanks to Dr. Lisa Ann Osadciw, my advisor and mentor. She has supported and guided me throughout this journey at Syracuse University. Her unwavering support and enthusiasm for my research provided the necessary motivation to successfully complete this dissertation. Dr. Osadciw was not only a part of our career goals but shared our personal moments. She has not only shared her breadth of knowledge, wisdom and experience but made us feel a part of her family. Some of my fond memories of Syracuse include picnics with her family at their home. I would also like to give a special mention to Walter Osadciw, Addie Osadciw, late Frosty, Sasha and Taylor.

I owe my sincere appreciation and gratefulness to Dr. Can Isik. He served as my co-advisor and mentor in the Future Professoriate Program at Syracuse University. His commitment to students is a legend in the engineering department at Syracuse University. He has always been warm and receptive of my needs and present to guide me through. His words of advice, teaching style and approach to student needs will be forever etched in my mind.

A special thanks to Dr. Jay K Lee for his continual support, guidance and advice. He played a pivot role in my doctoral candidacy for which I am grateful. His motivation and advice still resonate within me. Dr. Shoba Bhatia deserves a special mention for her work with Women in Science and Engineering (WiSE). Dr. Bhatia is a guiding light for young women innovators at the L.C. Smith College of Engineering and Computer Science. My gratitude and thanks to Dr. Makan Fardad who has shaped my teaching skills while serving as his teaching assistant. I wish to thank, Dr. Wenliang (Kevin) Du, for his continued support and guidance in my research work. His in-depth knowledge, enthusiasm and discussions in class on security have inspired my research.

I wish to share special thanks and mention to Dr. Yingbin Liang, Dr. Pramod Varshney, Dr. Fred Schlereth, Dr. Chilukuri Mohan, Dr. Romieu and the faculty at the L.C. Smith College of Engineering and Computer Science, Syracuse University. I extend my thanks and acknowledgment to the staff - Brenda Flowers, Barb Decker, Barb Hazard, Cynthia Bromka-Skafidas, Sue Karlik, Neil Jasper, James Spoelstra, Roseanne and Karen Pardee who have gone beyond their means to help me during my stay.

I wish to thank my group mates at DREAMSNet (Development and Research in Evolutionary Algorithms for Multi-Sensor Networks) Laboratory. My research ideas and progress would not have been possible without the stimulating research talks and collaborative work. Every research contribution is a DREAM come true at DREAMSNet.

An old indian adage, “Matha, Pitha, Guru, Deivvam” meaning “Mother, Father, Teacher and then God” is an apt saying implying the order of reverence one must consider. But I saved the best for the last and surely the most, I would like to thank my parents, P. Muraleedharan and P. Sreekumaridevi, I am indebted to their love and moral support they have provided me since birth. They have educated, financed and aspired me to chase my dreams and never to give up. Thank you and I love you! I have led my life by examples set by my brother M.S. Rajesh and sister M.S. Reshmi. I thank them for the joy, laughter, cheer and support they have provided me all my life.

Many years ago, I made a commitment and I ended up in the hands-on problem-solver, graphic designer, reviewer, stress reliever, soul mate and above all a beloved and devoted life partner, Thomas Silveira. I thank my husband for all his intellectual discussions, passion, support, patience and sacrifices made to keep my life focussed and in prespective. My life is meaningful with his presence and the joy of our love, our little baby girl. I thank my daughter, Reyna Silveira for her unconditional love, and kisses assuring me that there is more to life than just work and science. Its her energetic presence and smile that brings light to my day. Rey is the driving force in completing my degree and a new purpose in my life.

I have always wondered how incomplete life would be without the paw prints - Sonya, late Dolly, late Sweetie, and late Tiger, right from my high school days to now. Their wags and naughtiness have only added another dimension to my happiness. I also extend my gratitude to all my in-laws, relatives and friends who have played a crucial role in my life.

And finally to God with many forms I surrender, for all the blessings he has showered upon me.

CHAPTER ONE

Introduction

"Research is formalized curiosity. It is poking and prying with a purpose." - Zora Neale Hurston

This dissertation presents a security framework applied to a sensor network that can be managed by a cohesive sensor manager. The objective of this research is designing an evolutionary algorithm with controllable parameters to solve many security threats in a heterogeneous communication network. The performance of a sensor network is evaluated by efficient and reliable communication between the sensor nodes under adverse environments. This chapter stresses the importance of sensor network in our day-to-day life, and discusses the network's limitations. The performance of any application is based on the cost, reliability, efficiency and accuracy of the system, thus implementing an apt framework ensures longevity and security of the sensors. The proposed framework can be tailored to the sensor's resource availability and hence, can be used for applications using homogenous and heterogeneous nodes.

1. 1 Sensor Network

The evolution of sensor technology has a tremendous impact in the new millennia. The need to monitor, sense, track information in different environments using cost-efficient communication had lead to exploration of every layer of the sensor architecture. There are different types of sensors such as pressure, seismic sensor, heartbeat monitor, etc. The sensor types implemented are primarily dependent on the application or user requirements. In wireless sensor network (WSN), sensor nodes made of radio frequency (RF) communication links are deployed over a vast area. There are ongoing research on optimal deployment of sensor nodes[1, 2] assuming that the sensors are homogeneous and thousand of sensors are deployed. The tiny, inexpensive sensors have limited memory and functionality given the fact that the batteries(y) have limited power supply. The functionality of the node is to sense, collect and distribute the dynamic information from one sensor node to another. The important characteristics of a sensor network is scalability and reliability, as more than thousands of nodes can be deployed. The sensors deployed under harsh environmental conditions, are affected by electromagnetic interference (EMI) and thus communicating uncorrupted and secure messages without delay in a lossy wireless medium becomes essential.

1. 2 Limitations: Sensor Network

The traditional issues of a wireless network are energy conservation, bandwidth, data rate requirements, stability, scalability, QoS, real-time adaptation, location awareness, reliability, mobility and cost. Whereas wireless sensor node is limited to two main resources namely, energy and bandwidth. Energy consumption plays a key role on the survivability (lifetime) of sensors [3]. Performance of an application is mainly based on the system requirements, the following characteristics of a network directly hinders the performance parameters chosen.

1.2.1 Network Architecture

There are different ways of modeling a network, such as hierarchical, cluster-based, distributed and hybrid. In some applications sensor nodes act in a distributive manner without any centralized control such as, Fire detection, Evacuation plans etc, where the occurrence of an event is triggered based on its priority. The distributive architecture would enable parallel communication but also might lead to redundant packets (messages), hence optimal message transmission is required. This type of architecture is best used in applications where time constraint of messages is the primary concern, such as Health monitoring, Disaster Evacuation, etc.

In a Hierarchal architecture [4] the communications between nodes are carried in an orderly manner. The base station or a monitoring system queries to any region of interest and receives responses from the nodes. In a hierarchal architecture, applications that require central processing with decision making abilities, in some cases human intervention is required. Applications such as Traffic monitoring system, Building monitoring system, Maintenance applications i.e., Gas pipeline repairs, Windmill repairs etc.

In a Cluster-based architecture [5] every region is partitioned such that each has a cluster-head (CH), which aggregates the data and acts as the relay node for transmitting information, thus saving energy. These cluster-heads are frequently updated to ensure lifetime of the sensors. The process of choosing a cluster-head requires communication and synchronization between peer nodes, thus leading to energy consumption. Cluster-based architecture is best suited for applications that are data driven such as Biometric Identification system, Traffic Monitoring system, etc.

A Hybrid architecture [6] is one which is a combination of any of the above. In recent research, a combination of event based and data driven applications are used, for e.g., in Air traffic monitoring system, there is a huge amount of flight information used which needs to be fused and also events such as terrorist attack comes along, then emergency facilities needs to be accounted. Thus an architecture of a network changes is one of the parameters that would affect the performance of the system.

1.2.2 Deployment

In practice, deploying a sensor network in a hostile environment is done by random distribution or Gaussian distribution [7]. Therefore, it is difficult to know the apriori topology of sensor networks. In such cases, an approximation is made regarding the location of the sensors. There are many localization techniques proposed, such as Multilateration[9], Signal strength approach, etc., Since the exact location of a sensor is hard to estimate, any security threats occurred due to denial of service attack such as a Sybil attack cannot be identified. There are various methods of establishing encryption keys within neighboring nodes are used for securing the links, which is out of the scope of this thesis. Deployment and locating the sensors is an important aspect of any application.

1.2.3 Characteristic of Sensor Node

The characteristics of a sensor has major impact on the parameter settings of an application. The tiny sensors by nature have energy constraints, limited memory and are bandwidth deprived; hence a better knowledge on sensor's characteristics helps in building a highly robust and competitive application performance.

1.2.3.1 Energy Availability

Need for tiny sensors has lead to power restrictions on the devices used to built a sensor node and has also driven the cost. These sensors are small in size and are battery operated, therefore have limited capabilities. These sensor nodes can be used to relay messages and require neighboring sensors to communicate messages to distant base stations or destination nodes. As the sensors are deployed in hostile environments, replacement of batteries is not an option. Typically sensors consumes energy even when they are switch from sleep to active mode, hence each state of a sensor will contribute towards energy dissipation. Therefore, minimal usage of power can ensure the lifetime of the sensors.

1.2.3.2 Memory (Computation Power)

The reduced size of the sensors with limited power source also denotes computation constraints. In many cases, the sensors not only act as relay nodes but also fuse data to make optimal decisions, under these circumstances computation power used by any source is of great concern.

1.2.3.3 Adaptivity

There can be multitude of sensors deployed in a vast area, due to their limited power supply many sensors fail to perform in any stage of the application. The network performance should not be degraded due to any sensor failure such as technical faults, energy scarcity, malicious behavior, etc. Thus a good adaptable protocol design which is frequently updated with the current network topology would be best suited for a network deployment in harsh environments.

1.2.3.4 Scalability and Reliability

Any network needs to be scalable, for e.g., after initial deployment if the necessity arises for more sensors in a network, then the existing network structure should be able to accommodate newcomers (sensors). The process of adapting to the nature of the network by protocols is best suited for any application. A reliable communication is when the nodes communicate any message to the destined nodes with minimal interrogations from neighboring nodes. A equally weighted scalable and reliable network increases the performance of a sensor network application.

1.2.4 Security

One of the major concern of any wireless network is ‘Security’. Due to the above mentioned characteristics and limitations of sensor resources, traditional security schemes such as public key infrastructure (PKI) and cryptography cannot be directly applied. Any commercial or military application such as health monitoring and border protection involves time and data sensitive information communicated over public wireless medium. This information attracts intruders both to posses and falsify information that can lead to catastrophic events and human casualties. Thus securing network using minimal and energy efficient schemes without jeopardizing the network performance adds a layer of complexity to the existing problem.

1. 3 Wireless Sensor Network Applications

“Wireless Sensor Network is a boon to both industry and academia”. Current research in technology has increased the production of wireless devices with reduced cost and better performance that can be applicable to very large network with minimal human interference. The following examples gives a brief knowledge of the investments made in implementing wireless sensor network (WSN) in real time projects.

1.3.1 Applications - Industrial

Intel Research is working with the academia in exploring the challenges faced by sensor network. Deployment of WSN to monitor the health of semiconductor fabrication equipment is underway. Another application known as IrisNet is an architecture and system for a worldwide sensor web. It is modelled to help drivers locate available parking spaces near their destination. One other application by Proactive Health research lab in Intel is to conduct home heath care and aging-in-place technologies, which improves people's health by reducing nation's overwhelming healthcare bill.

Many Oil and gas companies are analyzing and developing WSN technology to increase production, streamline operations and reduce expenses. It is estimated that the oil industry would spend $200 million on WSN over the next three years, according to ON World. The largest multinational oil and gas companies are pilot testing mesh WSN using IEEE 802.15.4 radios. Monitoring the progress and maintenance repairs are the tedious and most time consuming job, by implementing WSN, the revenue of this industry could be increased.

Boeing, Endevco and Georgia Tech built a smart sensor based devices to measure pressure distribution across the surface of an airplane wing. The project is underway and still in its stages of implementing techniques for successful smart sensor network technology.

1.3.2 Applications - Academia

AWAIRS [10] is a project developed as a joint effort by UCLA and, Rockwell Science center. The network protocols and cooperative processing algorithms are incorporated to perform flexible tasks as small unit operations preserving energy and performance. The main goal of AWAIRS is to attack power management in all areas by trading off system performance.

Wireless Integrated Network Sensors (WINS) [11] has been developed by UCLA and Rockwell Science center. WINS is a commercial project, developed based on the MEMS technology with an embedded sensing intelligence.

Smart Dust [12, 13] (Autonomous Sensing and Communication in a Cubic Millimeter) is developed by U.C.Berkeley. It is used for both commercial and academic purposes. The Smart Dust project demonstrates the integration of sensors and communications into a cubic millimeter packed system. This involves both evolutionary and revolutionary advances in miniaturization, integration, and energy management.

A remote ecological network called PODS is built to investigate localized growth of endangered species of plants by University of Hawaii. MAC layer technique is based on 802.11b and Bluetooth, while the network protocol developed is Multi-Path On-demand routing (MOR). The data collected by the sensors consist of both weather and image, and can be accessed by users via Internet.

In MIT, WSN is applied for Environmental Monitoring in the Boston Botanical Garden [14]. CodeBlue is a scalable software infrastructure developed by Harvard University, where wireless medical sensors are used for medical care including pre-hospital and in-hospital emergency care, disaster response and stroke patient rehabilitation [15].

There are several sensor based applications in their developmental, demonstration or production stages that are very data sensitive where security of the data, network and the application is of great concern.

1. 4 Limitations & Security Challenges: Sensor Network

Security is a major concern that are seldom researched during the design phase of a protocol. Therefore, any new security approach should be compatible with both existing and upcoming protocols and technology. The following limitations and challenges faced by sensor networks,

1. Sensors have limited energy, bandwidth, computing power and memory.

2. Sensor have no physical tamper resistance.

3. Network can be deployed in harsh environments or unsupervised conditions.

4. Sensor share information using unreliable or open unsecure wireless medium.

5. The functionality of a sensor node varies with time i.e. sensing, computing, routing and idle.

6. Heavy security computation cannot be performed at the node i.e. security certificates and verification.

1. 5 Research Motivation

Routing algorithms are the backbone for data flow from source to destination while maximizing global network performance. Unfortunately, due to minimal or no communication security schemes, the data, link and the sensor node can be easily tampered by intruder attacks. Since, traditional security protocols are application dependent, they cannot be applied for sensors that are limited in resources. Also, security framework should be adaptive, reliable, scalable, resource and time sensitive while being independent of the network architecture and application. Unfortunately, protocols works best if they are tailored for a particular application. Hence, the need for security framework that is versatile, de-centralized and self-organized is immediate. A framework that can be customized for applications with minimal changes in controllable parameters to ensure user and application security is critical for day to day adoption.

1. 6 Research Contribution

The new era of commercial and military applications require heterogeneous network. Hence, a simple framework that can support security based on situation assessment is best suited for chaos and harsh environment. The simulated scenarios of this dissertation show that Cognitive Security Framework (CSF) is best suited for both homogeneous and heterogeneous sensor networks. Any framework works best, if the correlated or orthogonal performance parameters are carefully considered based on system goals and functions. The contribution of this dissertation is as follows,

1. Security vulnerabilities faced in every layer of sensor network.

2. A survey on the different security defense mechanism proposed by researchers for sensor based network.

3. The evolution of Cognitive Intelligence, which combines three major concepts Ant Colony Optimization, Partially Ordered Sets and Bayesian Network.

4. Design ‘Cognitive Security Framework’ (CSF) that can ensure security by adapting based on network type, architecture and application requirements.

The proposed, CSF is de-centralized, robust, self-organized, scalable and independent of application and network architecture. The level of security can be tailored based on user and network requirements using controllable performance parameters. The CSF is designed to secure a network as follows:

1. Defend against Cross-layer Denial-Of-Service attack for existing protocols,

2. Detect and predict intruder attacks using sensor's attributes, using Bayesian network, and

3. Trace and isolate attacker based on intruder behavioral patterns using 'bait' architecure.

The energy efficient cross-layer cognitive security protocol (C2SP) defends communication link between nodes during Denial-of-Service attack by re-routing data through secure nodes. Develop a resource-aware feature in C2SP that enables data confidentiality, authenticity, integrity and authorization using simple features of the node. Develop a framework based on application cost and time that analyses behavior traits of intruder and traces using low and high 'bait' interactions. The dynamic nature of CSF makes it robust and suitable for applications where passive and active attackers are involved. The efficiency and optimality of proposed CSF is analyzed based on the quality-of-service (QoS), reliability, reduced false intruder detection rate and response time under varied security threats and harsh environmental conditions.

1. 7 Dissertation Structure

The remainder of this dissertation is organized as follows. Chapter 2 discusses the security vulnerabilities such as Denial-of-service (DoS) attacks, intrusion and anomaly threats that affects the efficiency and reliability of any sensor based application. The proposed Cognitive Security Framework (CSF) consists of three folds, in Chapter 3, the cross-layer cognitive security protocol (C2SP) that acts as a defense mechanism against single or multiple DoS attack is explained using Health monitoring and Emergency Responder application, where heterogeneous links are used. In addition, the C2SP has the ability to store information for future analysis, and can be utilized using data mining techniques. The feature of Bayesian Network as a feedback in the C2SP to predict attacks using security metrics is explained in Chapter 4. Bayesian based approach is applied on vehicular ad-hoc network to verify the performance and relibability of the algorithm by identifying the jammer DoS attack and also locating the jammer using multiple observations. The final phase of CSF, which predicts and traces intruders based on their behavioral patterns for applications, where cost and security is uncompromisable using 'bait' architecture is explained in Chapter 5. The battlefield monitoring application is simulated to evaluate the performace of the proposed approach. In addition, the the validity of the attack and the ability to detect new DoS attack is also discussed. The three-fold framework is presented with application-specific simulations that emphasizes the outcome of security measures taken to attain better network performance. Chapter 6 concludes with research analysis and the possible extension of the proposed framework to any future application specific security problems.

CHAPTER TWO

Sensor Network Security

"Security when best applied is an application's medallion, otherwise an adversary's wit"

Unfortunately, many sensor network systems developed so far have lacked security during their initial design phase, paving way for researchers to interpret various intruder actions and security breaches that reduced system and application performance. Unlike traditional wired networks, modern nano-technology networks require security at each stage of communications. A single attack could jeopardize partial or full coverage in any network. Hence, an in-depth knowledge of the application system, hardware and software helps in designing appropriate and efficient security measures. In this chapter, various attacks that can be carried out in a heterogeneous sensor network are summarized, and existing approaches to securing sensor network and their limitations are discussed. Although each idea presented is a solution given a set of assumptions, the common end goal is avoiding an application from catastrophic breach by adversaries.

2. 1 Sensor Network Security

There are several research work conducted in field of security ever since the development of networks, but they cannot be directly applied to sensor network due to their resource constraint. A security solution should be scalable, adaptable, reliable, and resource efficient irrespective of deployment and environment. The security measures are based on entities such as,

1, Data (Information) security,

2. Network security and

3. Application security.

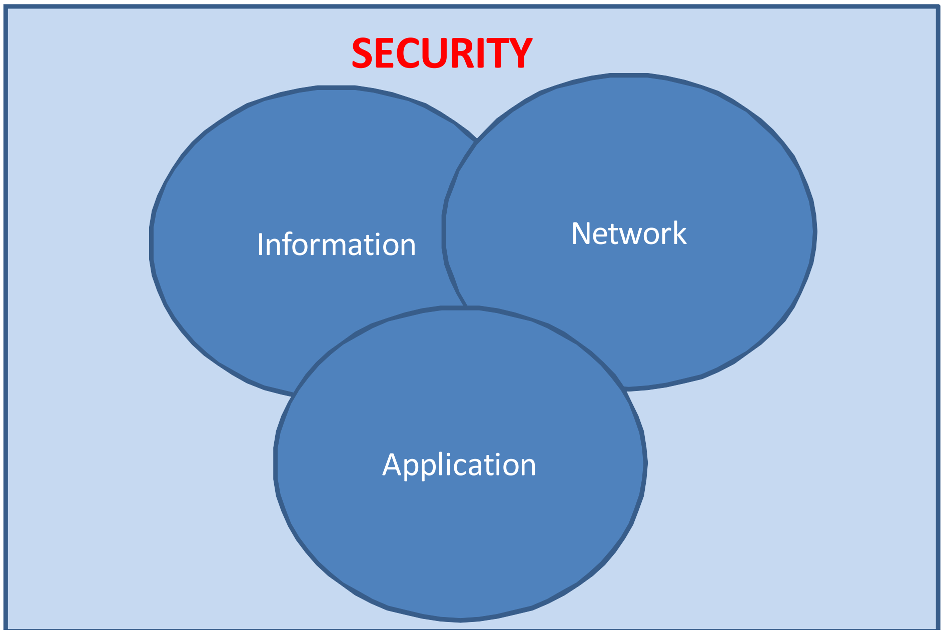


Figure 2.1. Three entity of Heterogeneous Sensor Security

A security framework that can accommodate threats from all the above areas as shown in Figure 2.1 and adapt to all environment is rarely found. Recent development in technology has led to a new era of heterogeneous networks, where resource-constraint nodes and pre-existing nodes needs to co-exist. In this chapter, we analyze all three aspect of security threats with respect to wireless sensor, wired and mobile nodes.

2. 2 Data Security

Data security is the fundamental concern of any application. Since, wireless network uses RF links to communicate between nodes, data is sensitive to attacks caused by environment, insider and outsider attacks. The four basic means of protecting data that existed in traditional wired and modern wireless network are Confidentiality, Integrity, Authorization and Authentication and in short termed as CIAA. Apart from these four, ‘data freshness’, ‘reliability’ and ‘availability’, vital attributes of sensor network is also included.

2.2.1 Confidentiality

The process of ensuring the data is accessible and relayed only by reliable and reputable nodes or user is called confidentiality. In applications such as emergency responder, Fire detection etc., data shared by radio through the wireless medium is highly sensitive and requires encryption. Since, sensor network are often used for mission critical applications, recharging batteries may not be an option. Hence, traditional public key cryptography or tedious complex security schemes cannot be used directly and require simple solutions.

2.2.2 Integrity

Data integrity ensures tamper-resistant from malicious nodes. Since, sensor network are deployed in open and harsh environment, the integrity of data sensed is constantly scrutinized and tested.

2.2.3 Authorization

In this process, a node is authorized to send information across the network when requested by a base station or user. This method of data authorization indirectly reflects a hierarchical structure within the network, and is mostly found in sensor based mesh network. Unfortunately, there are a few shortcomings in this authorization process, such as the difficulty in maintaining authorization for continuously growing network.

2.2.4 Authentication

The source node during information transmission authenticates its data, which assures the originators identity and integrity and reduces tampering when relayed to sink node. A message is authenticated using reusable message authentication code or other schemes at each hop or a cluster of node depending on the application.

2.2.5 Data Freshness

An important feature of sensor network is data freshness. Therefore, any scheme should ensure both resource efficiency and high response time, as sensor based applications are also time sensitive. Any delayed data is not valued in sensor based applications, thus a time-stamp that relates to data freshness is used, which also helps in sensor localization.

2.2.6 Reliability

Data reliability is an important aspect of the information collect from various nodes in a network. Due to environmental conditions such as scattering, dust, walls, rain, heat, etc sensed and transmitted data become unreliable. Thus, methods used to obtain reliable data is vital for applications where heterogeneous network is involved, as it affects overall application performance.

2.2.7 Availability

Data or information needs to be available to all nodes and users that are deemed legitimate and hence it closely relates to authorization. But, if the participating node has resource availability, the data when requested needs to be transmitted from source to destination. Therefore, a sensor's service or reputation is based on the number of times its data is made available to the genuine user to the total number of message transmission request.

Data security is a challenging task for heterogeneous networks as proposed schemes should be adaptable for all environments and maintain system performance. Also, the features of data security discussed above require tailoring for the sensor network due to resource constraints.

2. 3 Network Security

Modulation, coding, routing protocols, medium access control (MAC) protocols and localization algorithms designed for sensor networks directly contributes to resource availability and application performance. The shortcomings of security schemes has led to attacks such as Denial-of-Service (DoS), intruder attacks, privacy and identity thefts. Another major concern in sensor network is identifying if a node is genuinely under attack. As nodes can either deplete its resources or become unavailable, this can be misinterpreted as being under attack. Thus, evaluating and maintaining sensor's resources and security claims ensures the application's longevity and reliability.

2.3.1 Denial-Of-Service Attacks

DoS attack occurs when a node is deprived of its service to the application irrespective of resource availability. DoS attacks can easily affect both sensor and network performance if one or more sensors are compromised. There are several types of DoS attacks such as jamming, collision, black hole, etc as shown in Figure 2.2. Sensors are more vulnerable to single and combined DoS attacks, for example a worm-hole and flooding attack when combined can lead to misleading information and packet loss. Thus, genuine nodes that constantly attempt to transmit data unaware of its neighbors current status can lead to resource exploitation. There are many concerns that arise from DoS attacks, such as

1. Sensor's quality of service
2. Application's response time
3. Node's resource availability
4. Insider/ Outsider attack
5. Application/Sensor downtime

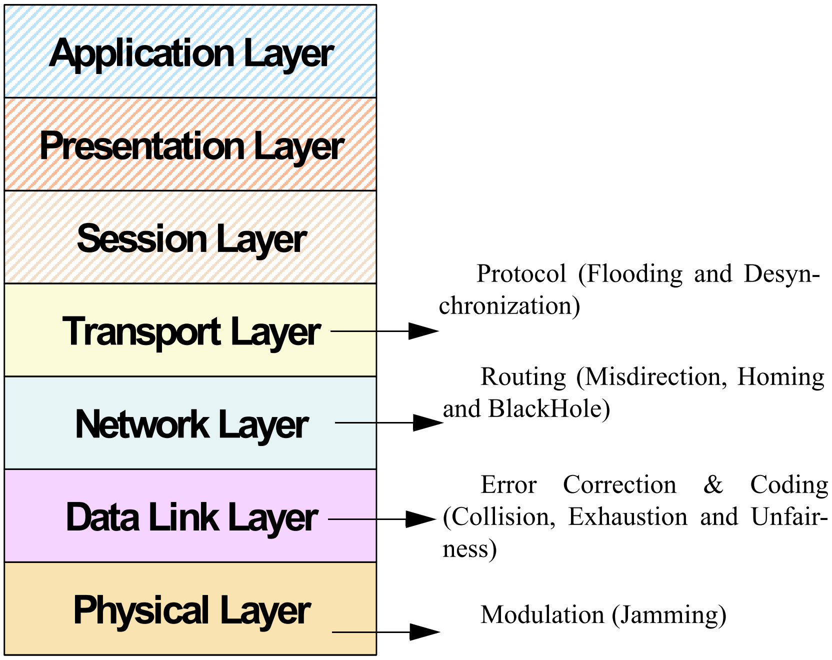

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Protocol (Flooding and Desynchronization)
Routing (Misdirection, Homing and BlackHole)
Error Correction & Coding (Collision, Exhaustion and Unfairness)
Modulation (Jamming)

Figure 2.2. Denial of Service Attack on Sensor Network Layer

Hence, protocols or methodologies applied to detect DoS attack need to consider node's status to better judge if its under attack or has depleted its resources. The different layers of the sensor network's Open System Interconnection (OSI) model that can be affected by DoS attack are physical, MAC, routing, and transport layer. Figure 2.2 associates the type of attack that occur and the OSI sensor network layer [16, 17]. The blocks that are shaded in stripes can be eliminated, as it primarily depends on the kind of protocol that is used for sensor network.

2.3.1.1 Physical Layer

Nodes of heterogeneous networks are a combination of wired, and wireless communication, but limitations exist in terms of energy and bandwidth. In the physical layer, 'jamming' attack occurs due to multiple sources of radio frequency (RF) interference that can be both unintentional and/or intentional due to neighboring systems, the environment and malicious nodes. It is the most vulnerable attack [18], as it blocks all communication in such a way that either the node is permanently set in a sleep mode or runs out of energy trying to overcome the interference. Thus, the network is denied from its functionality. The effects of a jamming attack depends on the type, location and noise power of the jammer.

Apart from jamming, one other physical attack that can be caused to any network is 'tampering'. Intruders can easily tamper when sensors are deployed in remote or harsh environments as they are rarely monitored.

2.3.1.2 MAC Layer

The MAC layer is the backbone connecting two different nodes to communicate. Hence, ‘collision’ attack due to a poorly executed data exchange may lead to the acknowledgement (ACK) message becoming a collision attack. Thus, under collision attack the probability of losing packets is very high affecting the reliability of the application. In addition, ‘exhaustion’ incinerates the resource availability at the node making it cumbersome for future communication. The MAC layer is primarily responsible for setting message priorities, which if done incorrectly can lead to ‘unfairness’ attack. In this attack, genuine nodes with the least priority never gets service irrespective of resource availability.

2.3.1.3 Network Layer

Network layer is the foundation of routing protocols for communication between source and destination. In sensor based networking, minimal routing means minimal delay which, in turn contributes to ‘data freshness’. But due to the lack of simple security features in the routing protocol, ‘misdirection’ can easily occur where the message is redirected to any node but the destination. Thus, exploiting the source and participating (relay) node’s resources. A greedy routing protocol tends to neglect nodes with genuine traffic in its route due to its greediness and prioritizing its own messages contributing to ‘greed and neglect’ attack. Routing protocol that works based on advertising from neighbors can lead to the ‘black hole’ attack, where both the neighboring and advertised node exploit resources by actively participating in routing information.

2.3.1.4 Transport Layer

The communication between two nodes is managed using transport layer exchanges maintaining an end-to-end connectivity. The ‘flooding’ attack commonly occurs in this layer, as multiple requests for resource allocations that end abruptly would lead to exploiting resource of the genuine node. Since nodes require synchronization, a ‘desynchronization’ attack by a malicious node can lead to repeated retransmissions of messages leading to resource exploitation.

2.3.1.5 Other DoS attacks

In a Sybil attack [19 , 20] an illegitimate node presents multiple identity thus deceiving its neighboring nodes. In a worm-hole attack, the packets are tunneled to another location and re-sent to bombard the network with communication overhead, thus reducing the QoS. Sinkhole attack, is one where compromised node attracts traffic from neighboring nodes. Selective forwarding is another DoS attack, where nodes rather than broadcasting messages choose to forward messages and only a fraction of message received.

Since all the above attacks primarily depend on the various layers of the protocol, incorporating the performance parameters that contribute towards increasing QoS in the network is used to obtain an optimal and secure route.

2.3.2 Intrusion Detection

Intrusion detection system (IDS) is an important part of securing the network against abnormal behavior. In some network, IDS is either centered within a cluster or performed at base station. IDS can be used to detect and predict attacks using predetermined or learning strategies. The level of intruder detection and tracking depends primarily on the application's resource availability and time.

2.3.3 Secure Data Aggregation, Localization, Communication and Routing

Other challenges faced by sensor network are data aggregation [21], communication, routing and node's localization information. Many applications are deployed in open environment where external attacks are very common. Hence, an existence of secure link enhances authorized nodes and data transmission, but would require aprior knowledge or a learning algorithm for sensor network management.

2.3.4 Key Establishment and Privacy

Data security measures in WSN are vital as information used can be very sensitive depending on the application. Since sensors are so tiny, storing and accessing traditional key schemes such as Public Key Infrastructure (PKI) and other (symmetric and asymmetric key) requires high computational power, memory and energy. Hence, the key establishment strategy helps in achieving data security for nodes, and reduces Sybil attack [22 , 23]. Data privacy can be maintained in numerous ways, but efficiency and reliability based on application needs is essential. For example, in an indoor security system, user's biometric data is used both for authorization and private key for authentication. Unfortunately when the key is compromised the user identity is jeopardized.

2. 4 Application Security

Security based on the application is primarily responsible for the end user or system performance. Thus, any protocols, architecture or methods designed based on the application's constraints, make it unique. The feasibility and adaptability of the proposed approach should have a certain tolerance level to co-exist with other technology. Many recently designed application specific methodologies seem to have security features for each layer, which are inconsiderate in terms of the computation complexity, and resource exploitation.

2. 5 Existing Security Solution against Attacks

Many recent research advances in the field of security for sensor networks categorize based on information (data), service and application. There is no solution against physical tampering of the nodes i.e., side-channel attack using power analysis can be attempted easily [24]. Also, when sensor based applications are deployed in remote locations, nodes are vulnerable to both environmental or attacker induced noisy data. In addition, in certain applications where node data is available via Internet for remote applications are susceptible to software attacks prevalent in any wireless applications. The proposed solution given below can either detect or countermeasure a single attack.

2.5.1 Security Against Information

In data security, existing defensive security measures include schemes such as data authentication, key establishment, public key cryptography, etc. A pairwise key is managed in Low power Energy Aware Processing (LEAP) [24 , 25] between two nodes, but neighboring identities need to be established and maintained while all nodes are considered to be trusted links. In μTESLA (Time Efficient Stream Loss-tolerant Authentication)[26] a key chain distribution with asymmetric key helps reduces the disclosure of symmetric keys by the sender. The only limitation of this scheme is the sender requires a unicast communication to each sensors. A modification to µTESLA proposed by Liu and Ning [27] uses the symmetric key method, where multilevel key chain distribution with predetermination and broadcasting is used. The protocol allows disclosing keys at a time interval and the base station also broadcasts disclosed key and initial bootstrapping for new nodes to conserve energy. The µTESLA protocol assures that even if a single node is compromised, the network is secure. Jolly et al proposed a key management scheme that relies on probabilistic key sharing with hierarchal links such as gateway. SNEP (Sensor Network Encryption Protocol) [28] provides security characteristics such as data confidentiality, two-party data authentication, authorization and message freshness using a low communication overhead of 8 bytes per message. Since the message is encrypted uniquely each time, it is assumed to prevent eavesdropping.

In [29] Kong et al proposed a threshold secret updates and certificate security based on public key infrastructure (PKI). Zhang, Zhou and Yang [30] use node-to-node authentication that accommodates the pairwise keys with neighboring nodes. Ouyang et al [31] proposed a hashing-based ID randomization (HIR) and Reverse HIR. The HIR is applicable for sensor anonymity, while RHIR is used when the key is compromised in a network. Therefore, RHIR requires more storage for the hash data and higher computation.

Hence, researchers contributed schemes such as TinySec [32], SPINS that claim resource efficiency and application longevity. Security in TinySec is established using traditional link layer encryption and authentication such as RC5 or SkipJack ciphers. But, due to the mathematical crypter operations, network overflow and high packet loss is encountered. Also, TinySec uses private key cryptography that leads to integration of key distribution, key management and digital signatures techniques. Recently, elliptic curve cryptography (ECC) is used in TinyOS to distribute keys.

One other approach to data security is homomorphic schemes that helps in achieving both data aggregation and confidentiality between one hop nodes, but they are computationally expensive, time consuming and lack in-network verification for compromised aggregators. Data integrity is attained by hop by hop key management techniques, where malicious node is not included in data aggregation. But, there is no such scheme to assure aggregator node is itself under any threat for unattended sensor network. Some researchers propose node reputation [33] and data origin authentication methods for data integrity.

The main drawback of all the above mentioned protocols are computational power, since sensor nodes are tiny and can store only limited amounts of energy, using assigned bandwidths and restricting computational cost. Although the protocols promise secure communications, they fail to accommodate the basic features of sensors. Data security is a challenging task, although there are many security schemes addressing data integrity, freshness, confidentiality and authentication. There is on going research in combining all the features of security in a single security scheme without jeopardizing application's resource and availability.

2.5.2 Security Against Sensor Service

Any network requires un-disrupted service irrespective of its deployment, environment and resources. Sensor nodes in unattended environments can easily be subjected to attacks by malicious nodes that can disrupt both quality and service. Disrupted service to a node can be both intentional and unintentional, which can directly affect the network capacity and quality of service. DoS attack as discussed previously affects the reliability of the information, making detection of a DoS threat more crucial than recovering from the attack. Every layer of the network is vulnerable to attacks such as jamming, collision, misdirection, flooding, etc., In crucial applications such as disaster relief, health monitoring etc., reduced performance due to DoS will make the network unfit for the application. Hence, detecting DoS attacks and defending the network by taking the necessary countermeasures helps in maintaining or improving the performance of the application.

Interception or compromise of the secure information by an enemy is an act that cannot be neglected. Hence, appropriate security measures need to be taken at every layer of the protocol design. Many attacks are caused by intruders who seldom have complete knowledge of the protocol. There have been several research conducted on the different kinds of potential DoS attacks on sensor networks. Wood and Stankovic in [34] had summarized different DoS attack and its effect on the sensor network. Though no defense mechanism was proposed in the survey but different possibilities to reduce the effectiveness of the attacks were provided. In the physical layer, spread spectrum is often used to minimize the impact of a jamming attack. I conclude that due to limited resources code spread, as used in mobile networks cannot be used in WSN.

Channel hopping and physically moving away from a jammer is proposed by Xu et al in [35]. The approach primarily focussed on determining the occurrence of jamming but fails to investigate on the amount of overhead in channel hopping and jammer scanning, which is vital for sensor network.

In JAM, a mapping protocol for nodes that surround a jammer was proposed. Using this approach, the protocol creates awareness in the neighboring nodes to detect a jamming attack using message diffusion. Also, in this paper single-channel wireless communication was assumed. It was simulated using GloMoSim simulator with different range of jamming attack and neighboring nodes. The protocol was robust, when a message was rerouted, only data loss occurred in inactive nodes. The JAM protocol had failure rates of 20-25% of mapping nodes from twelve neighboring nodes within communication range. DEEJAM [36] a link-layer protocol was proposed to detect stealthy jammers using Zigbee hardware. The proposed approach required an encoding scheme and suffered packet loss, due to frame masking, redundant encoding and packet fragmentation. Also, Tay et al in [37] proposed a link-layer S-MAC protocol to countermeasure jammer attacks using data blurting and schedule switching. Cagalj et al in [38] proposed worm-hole countermeasure for jamming attacks, where wired nodes and coordinated frequency hopping (FH) pairs were used to re-route messages. The shortcoming of the proposed worm-hole method was the need for deploying wired nodes and the need for synchronization of the FH pairs.

In [39], a solution for denial of sleep attack using G-MAC protocol was developed. Nodes will stay awake to receive transmissions if an authenticated request by the GS station was sent. Unfortunately, packet loss due to limited wake up time was not considered.

In [20], a Sybil attack on a network and routing layer of WSN was analyzed. The authors assumed that a sensor node communicated with its neighbors using half-duplex as a single RF transmitter with various possible radio channels. The process of identifying Sybil attacks was based on radio resource testing. Legitimate neighboring nodes are allotted a single channel for identity. This process of identifying a sybil attack cannot function if the spectrum is jammed. Hence, it would lead to a false identification of a sybil attack.

In [40] Chaum used anonymous connections to route information against traffic analysis. Wu [41] developed an on-demand position based private (AO2P) routing protocol, while Wadaa et al's protocol [42] promises energy-efficiency for coordinate system, cluster and routing structure for maintaining anonymity of network virtual infrastructure.

In [43], routing security in sensor network was analyzed and a countermeasure was proposed. Defense mechanisms for different DoS attacks such as spoofing, wormhole, sybil, selective forwarding etc., was given based on the assumption that using radio frequency alterations can be made to the data.

In much of the previous research work, DoS attack the transmission was either assumed secure or intruded but only for injecting wrong data. One of the major catastrophes of any network is becoming non functional or unable to communicate. This is the most adverse attack a sensor network can encounter. This attack can account towards node's inability to communicate in spite of sufficient resources.

2.5.3 Security Against Intrusions

Other than data and service threats sensor nodes are also threatened by insider, outsider and other miscellaneous intruder attacks. An intrusion can be caused by a trusted or malicious node within or outside the network under stealth mode. The primary goal of an intruder attack is to learn the patterns and simulate a glitch in the application, so that frequent insider attacks can be launched at leisure. There are many intrusion detection system (IDS) proposed for wireless and ad-hoc networks, but they cannot be applied to sensor network due to the known resource and time constraints. Security in sensor network is in its infancy stages where very little research has been initiated in intrusion detection.

Zhang et al proposed a intrusion detection scheme in [44] where every node participates locally and independently in collecting data. The node's movement and its routing table updates are traced to build a anomaly detection model. Upon detecting a malicious node, the local detector broadcasts the message to the network, and every node makes a final decision based on its neighbors report. But since, the local decision influences the overall security of the network, computation resources are very high if 'stealth' mode attack is injected by intruders. In [45] a multiple sensor intrusion detection system was proposed, where a cooperative detection algorithm was applied. A mobile agent with IDS system and intelligent routing scheme was implemented. This approach requires high computational and energy resources.

One other approach to intrusion detection can use game theory. In [46], an intruder minimizes the ability to get detected while the service provided maximizes the same using sampling (max-flow problem). Unfortunately, in real life sampling is expensive, and also the authors have assumed that the intruder has complete knowledge of the network. In [47], a cooperative packet forwarding framework was proposed. In this approach, static routes were assumed and behavior of nodes were tracked although a list was not required to be maintained. Roman, Zhou and Lopez in [48] proposed an IDS framework that can accommodate local and global agents to act as watchdogs, but unfortunately the nodes were considered static and there was no implementation of this work nor apparently further research to-date.

The above mentioned solutions contribute to security in data, service or intrusion. Unfortunately, there has been no framework designed that combines all the three phases of security that also balance resources and application reliability. Since sensor based applications require optimal solutions that maximize security, quality of service while minimizing time and resource availability. An efficient optimization algorithm is best suited to solve this non-deterministic polynomial-time (NP) problem.

2. 6 Multi-Objective Problem and Optimization

Sensor based applications involve multitasking, resource balancing while maintaining the user's services and security. The basic requirements of security schemes for sensor network are as follows,

1. Resource constraints
    a. Energy
    b. Bandwidth
    c. Memory
2. Computational complexity
    a. Distributed
    b. Cluster or Mesh
3. Adaptive
    a. Environment aware
    b. Application aware
    c. Resource Aware
4. Detection accuracy
    a. Reduced false positive claims
    b. Reduced transmission errors
    c. Reliable, Efficient and Optimal Solution

A multi-objective problem requires solutions that incorporate optimization techniques where resource constraints are minimized while maximizing performance. Evolutionary algorithms (EAs) and other techniques such as Ant Colony Optimization (ACO) [49 , 50], Invasive Weed Optimization Algorithm, Particle Swarm Optimization (PSO) [51], are famous approaches that derive from the genetic and simulated annealing methods. In the following chapter, we shall analyze the importance of ACO and its role in the proposed solution, Cognitive Security Framework (CSF).

CHAPTER THREE

Cross-Layered Cognitive Security Protocol

"A route can be long and tiring but definitely can be the safest, thou is Detour"

In the previous chapter, security in sensor network was formulated as a multi-objective problem. Hence, the need for framework that can balance and optimize resources while prioritizing security and application performance is essential. The three-tiered Cognitive Security Framework (CSF) is adaptive to applications depending on resource availability. The first tier, Cross-Layered Cognitive Security Protocol (C2SP), helps in detecting a threat and re-routing the message to the sink. In this chapter, a detailed analysis of the security protocol and its evolution is presented with application.

There are many algorithms found in literature to attain sub-optimal solution using meta-heuristic approach such as genetic, simulated annealing applied to travelling salesman, asymmetric travelling salesman, job shop scheduling, etc. Each approach possesses trade-off depending on the application or use. A critical selection criteria for an algorithm is reduced delay and the probability of obtaining an optimal and reliable solution. Ant Colony Optimization (ACO) algorithm is a learning algorithm with characteristics such as robustness and versatility that solves any NP hard problem. In this section, the background the evolution of ACO and its characteristics are summarized.

3. 1 Cross-Layered Cognitive Intelligence

Cognitive intelligence (CI) is derived from the biological aspect of swarm intelligence (SI). The learning rate of the proposed algorithm evolves over time. The performance parameters such as energy, optimal distance, packet delivery rate, packet loss rate and data traffic are weighed to achieve an energy efficient, secure and goal oriented network. The process of balancing resource constraint and obtaining a secure optimal route is NP hard communication problem. SI evolved as the collective behavior from a group of simple autonomous agents that work in a collaborative manner to achieve a common goal. The ACO algorithm utilizes the features of the ants (agents) in a real time environment. The agents (ants) in the system communicate interactively either directly or indirectly in a distributed problem solving manner. The following subsections gives a brief discussion on the evolution of the concepts used in cognitive intelligence and its key characteristics.

3.1.1 Evolution of Ant System

The natural adaptability of insects and other creatures to survive and thrive through cooperative behavior has astounded scientist and researchers enough to analyze the swarm behavior of ants, bees, and birds and attempt to artificially replicate it. In nature, ants set out to find food from their home cooperatively. A special group of forage ants are appointed with this task, who looks for food in a random manner. Stumbling upon an obstacle, the ants choose alternate routes to reach their destination (food). Over time, the ants find and share the best routes to destination. If anything changes in the environment to affect these routes, the ants simply adapt. The swarm behavior of the ants when implemented in engineering problems are capable of solving many complex, dynamic optimization issues.

3.1.2 Characteristics of C2SP

The three main characteristics of ACO are pheromone deposition, state transition probability and tabu-list, which are modified to incorporate “cognitive” intuition.

Figure 3.1 shows the agent traversing a maze interactively using low and high pheromone deposition. Upon finding an obstacle, the agents deposit low pheromones along the path warning others of the problem and move forward in their quest to find the destination.

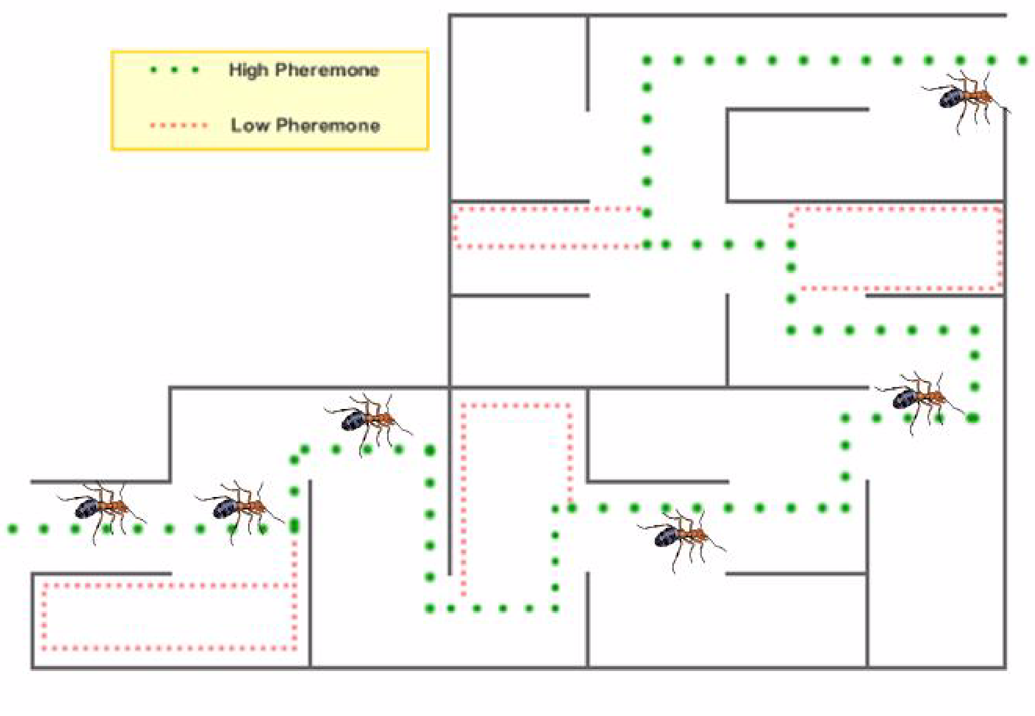


Figure 3.1. Agents traversing a maze [52]

3.1.2.1 Pheromone deposition

Ants traveling from source to destination interact with other ants using a chemical substance called ‘pheromones’. Similarly in the artificial ACO algorithm, pheromone deposition is implemented depending on the visibility of the ant. An agent is an entity capable of performing tasks autonomously using predefined behaviors or a set of criterion. In implementation of this approach in an application, agents mimic the swarm behavior of ants or other creatures. The pheromone deposition along a route increases as more agents traverse through the route. Also, the attractiveness of a route increases so that the probability that an agent takes a particular route increases. Agents move toward an optimal solution by sharing their knowledge with their neighbors. The initial set of agents deployed in the network traverse through all the nodes in a random manner. Each agent leaves trails by depositing pheromones on the route.

In C2SP pheromone depositions on the paths serve as a means of communication between the agents. The agents use the pheromones to help select the best route through the network. The most secure route is one that has the highest level of pheromone deposition. The performance metric is applied as the visibility criterion, and incorporated in the pheromone deposition function ψ by

$$\psi_{ij}(t) = \rho\psi_{ij}(t-1) + \frac{Q}{\eta_t} \tag{EQ 1}$$

where ψ is the pheromone deposition; i and j are the source and destination; (t-1) is the previous pheromone value; η_t is the visibility of the ant for an entire tour; r is the memory; and Q is an arbitrary value.

The pheromones on all paths are updated at the end of a tour. Thus, the route taken by the agent is both energy aware and time sensitive. A key feature of the proposed protocol is that the pheromone deposition (1) can be modified based on the performance requirements making it adaptive to any application.

3.1.3 State Transition Probability

The transition probability of an agent is defined as the probability taken by the agent to choose a particular node as its next hop towards its destination. Thus, the probability function (P) includes the performance parameters that impact the network, such as distance and energy,

$$P_{ij} = \frac{(\psi_{ij}(t))^{\alpha}.(\eta_{ij}(t))^{\beta}}{\sum_{k}(\psi_{ik}(t))^{\alpha}.(\eta_{ik}(t))^{\beta}} \qquad \text{(EQ 2)}$$

where ψ is the link cost function, α and β are the power on the pheromone deposition and cost function. The link cost function, ψ, is also based on the performance parameters. Hence, if the distance and energy are of primary concern, then

$$\psi_{ij}\text{=cost (D, E)} \qquad \text{(EQ 3)}$$

This cost function can be modified based on maximization or minimization forming a multi-objective min-max function.

3.1.4 Tabu List

A Tabu-list serves as memory tool listing the set of nodes that a single agent has visited. The agent's goal is to visit nodes in the network depending on the number of hops. This list helps agents to avoid looping that can occur during routing. In C2SP, the tabu list eliminates any redundant route traversals thereby conserving node's energy, and also an updated estimated energy availability in the nodes for the particular sub-optimal route with high reachability. Thus, the tabu-list supports energy usage prediction and decisions concerning situation assessment. The use of the tabu-list information for pattern analysis and will be discussed in the next chapter.

The pheromone deposition, tabu-list, and energy monitoring help this novel ACO algorithm to obtain an optimal solution and adapt during node degradation. These three modified characteristics can be tailored to any specific application making C2SP robust and versatile.

Success of an algorithm is defined as attaining the optimal solution. The computation time is defined as the amount of time the algorithm takes to obtain an optimal solution. In some cases, a combination of artificial intelligence such as a Bayesian network [53], and any of the EAs can achieve better results. A trade-off between factors affecting the overall performance of a system is primarily application dependent. The advantage of using EA is primarily because the population is searched in a parallel manner and not in a one-to-one basis. EAs do not require any derivative information or any auxiliary knowledge. EAs require only the objective function and the fitness level for performing a directive search. It uses only probabilistic transition rules rather than deterministic ones. Therefore, EAs are generally more straightforward to apply. EAs can provide a number of potential solutions to a given problem if all solutions produce identical performance. There exist possibility that EAs could lead to a pre-mature solution, but it's upon the user to define the fitness function in a way to obtain global optima rather than a local optima. In the following section the cognitive protocol adaptive to the security features is explained in detail.

3. 2 Cross-Layered Cognitive Security Protocol

There are tremendous advantages in deploying a sensor-based protocol, which will include self-adaptive and self-organizing behavior. The robustness and de-centralized features of the C2SP attains a feasible solution even during node degradation due to resource or attack. The C2SP's adaptiveness is based on the flexible cost function that can be modified to suite any application thereby making it a generic solution. A secure protocol can be designed only with in-depth knowledge of the application. Sensors are faced with many constraints namely wireless channel, quality of service, and energy efficiency issues.

3.2.1 Wireless Channel Constraint

The sensor communication through a wireless medium affects the quality of data transmission. The quality of information is affected in a sensor network application based on the following:

1. The nodes are half-duplex, thus cannot receive packets if node is in transmit mode leading to traffic congestion.
2. Wireless channel has noise, fading and shadowing that could deteriorate transmission.
3. Interference from neighboring nodes, can lead to packet drop.
4. Limited bandwidth restrict transmitting heavy data i.e., biometric
5. Propagation delay
6. Error in clock synchronization affects location information.
7. Error control strategies lead to heavy computation.

The protocol design should consider these constraints to improve the quality and quantity of information.

3.2.2 Quality of Service Constraint

Quality of service is an important factor in any wireless application as it directly affects the performance of the network. Traditional wired networks provide high reliable information without user convenience. Hence in wireless networks a trade-off between different parameters has to be attained in providing good QoS and reliable service. Also, the QoS varies dynamically based on the user's request. Hence, a weighing scheme tailored to each individual request would increase the QoS. The common parameters that are used in QoS are distance, energy, and packet delivery. In sensor based application, QoS cannot be judged based on packet drop, as nodes relay prioritized messages. Whereas, the frequency of packet drop by a node also relates to its reputation. Hence, careful consideration of the metrics that affect performance and reliability is needed.

3.2.3 Energy Efficiency

Energy efficiency impacts the lifetime of the sensors, which directly reflects the network lifetime. The energy level at each node needs to be tracked, and should be set with different threshold levels to avoid simultaneous node failures. Also, the sensors can communicate using different power control schemes, which allow them to use high energy level to transmit during priority events signal and switch to lower energy level for normal traffic. The use of thresholds at the node also helps in identifying the node's lifetime and its coverage ability.

3.2.4 Cross-Layer Approach

Every layer of a sensor network reflects the performance of the application. Hence a cross-layer approach that can work collectively to improve the QoS is preferred. There are also some potential risks in cross-layer design as discussed in [54] that leads to a 'spaghetti effect'. Thus an intelligent approach that has the learning ability to improve the reliability of network using cross-layer approach is designed and presented here using cognitive intelligence.

3.2.4.1 Salient Features

C2SP overcomes the constraints of sensor nodes by extending the ACO algorithm using partially ordered sets (POSets). POSets is a weighing scheme that helps in attaining multiple objective solutions using reinforcement.

There are different types of reinforcement namely positive, negative, penalizing and extinction. The positive and negative reinforcement helps to increase the strength of response, whereas the penalizing and extinction characterizes a weaker behavior. A reinforcement parameter is incorporated in C2SP to achieve global solution. In applications like Smart Grid, Health Monitoring, it is best to improve the learning behavior of the agents rather than penalizing or extinguishing the solution.

The performance of a system is affected due to improper and inflexible design structure. The salient features of the C2SP helps in achieving the following

1. Adaptive Modulation Scheme
2. Adaptive Error Correction Scheme
3. Adaptive Power Control Scheme

4. Adaptive Traffic
5. Adaptive QoS
6. Message Prioritization

The performance parameters such as energy, distance, successful packet delivery, packet loss rate and data traffic are weighed to achieve an energy efficient, secure and mission oriented network. The meta-heuristic cross layer protocol combines the factors that affect the performance in physical, MAC and routing layer to achieve maximized performance for using minimal resource thus achieving a multi-objective solution. C2SP is a hybrid algorithm that self-adapts, self-organizes and evolves to the network's needs. The salient features of the agents are combined with POSets which helps in attaining an application driven performance.

3.2.4.2 POSets

One of the major challenges in sensor management is providing a mathematical framework that can consistently represent the complex multidimensional optimization problem. POSets has been used in queuing theory, networking, and lately sensor management [55, 56]. POSets provides a graphical mathematical framework for representing relationships between a finite numbers of elements [57].

POSets formulates weights at each graphical level to flow down the importance of the performance parameter measuring the expected system goal. In sensor based applications, the performance is broken down to speed of alert, and downtime. Downtime is the percentage of time the system is not functional because a sensor node is depleted of energy.

The speed of alert is the response of the system based on the hops, distance and BER in receiving the message.

In Figure 3.2, the four levels to the mission POSet are illustrated. The performance parameters are weighed based on its importance. The initial weights are assigned by the user, and can also be automated based on previous analogies from agent's information. The flow down of weights i.e., the lower case variables on the arrows should sum to one from their source. The entire POSet begins with a value of 1 at the top. Then the arrows exiting that node should sum to 1 or $\sum_{k=1}^{2} x_k = 1$

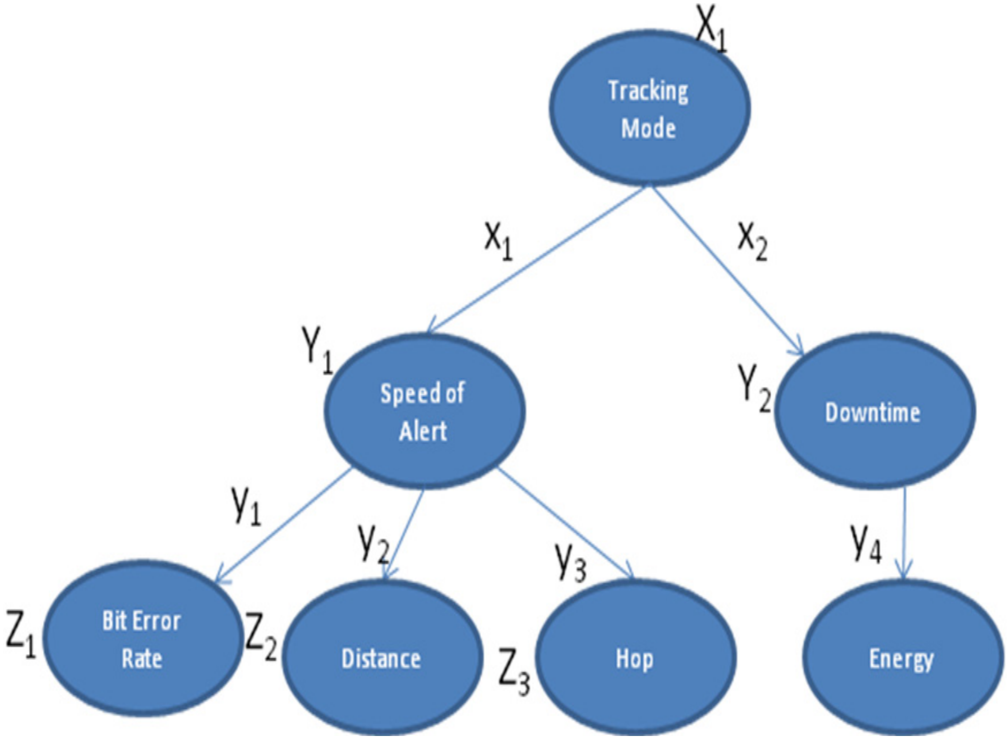


Figure 3.2. Illustration to support POSets computation.

The values of the next row of nodes is computed by multiplying the arrow's value by the preceding node or

$$X_1 x_k = Y_k, k = 1, 2 \tag{EQ 4}$$

The computation of the remaining POSet structure can precede in the same manner. The POSet provides a weighting scheme to guide the creation of a single global performance parameter so that sensor parameter decisions can be made by the sensor agents. For example, distance and the number of hops need to be emphasized if the sensor network needs to quickly send messages during priority queries or when distress events are sensed. Saving energy to prolong the life of the sensors is less important at that particular point in the system's lifetime. The weights are then computed from

$$W_k = Y_1 y_k, k = 1, 2, 3, 4, i = 1, 2 \tag{EQ 5}$$

The total performance is computed in for N parameters (N=4 here)

$$\sigma_{global} = \sum_{i=1}^{N} W_i \left[\frac{\left(\phi_{actual_i} - \phi_{required_i} \right)}{\phi_{required_i}} \right] \tag{EQ 6}$$

where σ is the global network performance parameter, and W_i is the weighting from the POSets structure in (5). The operator may make new decisions at this point as to the weighting applied in the POSet. These weights are then applied to the modified ACO algorithm to obtain the desired performance on the next system update.

3. 3 Sensor based Applications

Sensor based networks have developed in the recent years, and as discussed in Chapter 1 is found in our day-to-day life. Recently, the demand of pervasive sensor networks is extended to many real world applications such as health monitoring, habitat monitoring, emergency evacuations, etc. This process of wireless distribution of data helps timely updates and eminent measures under emergency situations. Unfortunately, there are also some challenges involved in providing cost and energy efficient application. The two main application addressed here is Health-care monitoring and Emergency Responder Network. Both these applications are heterogenous in nature, where devices vary in mission and requires coordination between sensors with limitations.

3.3.1 Health-care Monitoring

In the wake of ubiquitous technology, medical applications have taken a new road, where cure and treatment is found by mining information and providing global assistance. The main challenge of sharing sensitive data is patient's privacy, as there are policies ensuring data confidentiality but little can be done if a sensor is been tampered physically. Health-care applications process time sensitive data, hence transmitting the information using distributed, reliable and robust routing protocol becomes a vital role in any real-time application.

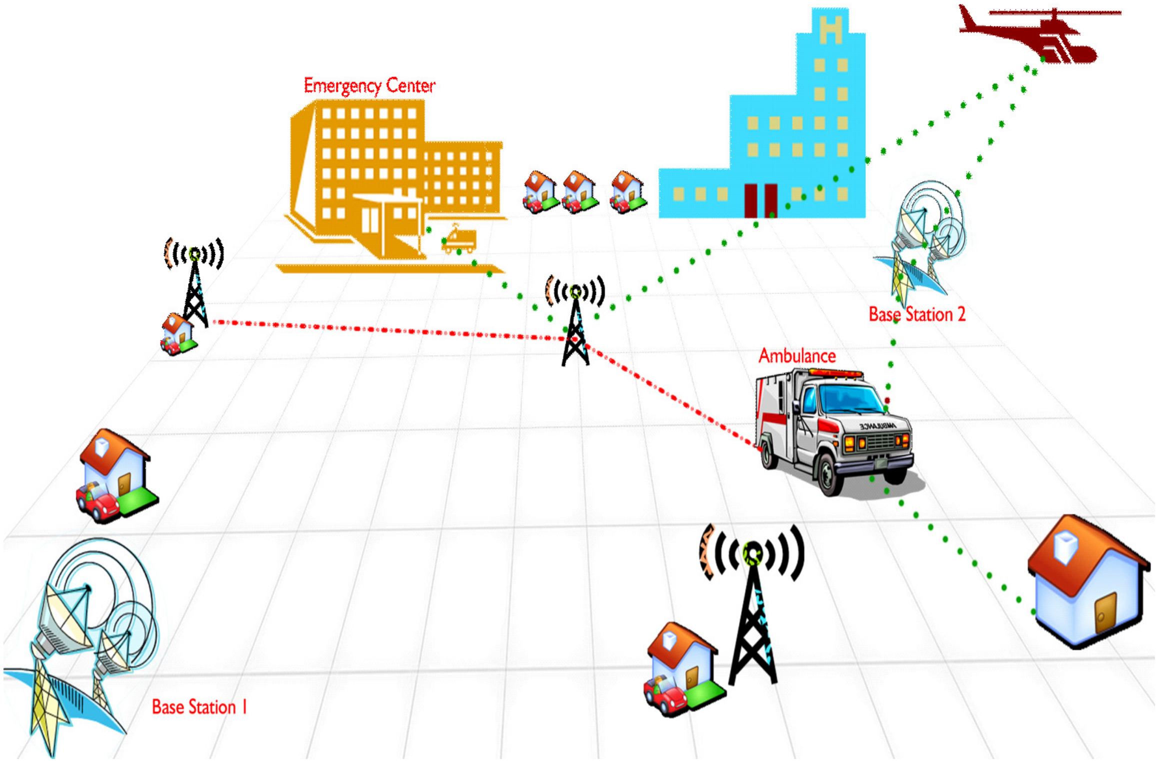


Figure 3.3. Sensor based Health-care Network

Figure 3.3 illustrates a health monitoring framework [58], where the nodes are spread in three forms, wired, wireless and mobile forming a heterogeneous network. A wireless node can be embedded on a patient in a non-intrusive manner to monitor his/her vital signs. While, mobile nodes can be placed on ambulances, where the emergency vehicles can either receive or send data to the nearest hospital or patient. The received data can be shared with individuals globally via web service to patient's caregivers, doctors, EMS, and nurses. The wired and wireless nodes are placed in the hospital where continued monitoring of outgoing and incoming patients with added functionality such as securing access inside building is also maintained. The data captured and transmitted are location, vital signs (temperature, heart rate etc) and biometric information. In this application, the data is collected continuously and by priority requests. Also, unlike fire monitoring applications where sensors data can be aggregated, in health-care every patient's data is unique and require varied care and hence, relevant

The assumptions made in this application are as follows,

- Some sensors are equipped with localization information and act as beacon for the add-on nodes
- Energy source on the beacon nodes are never drained.
- Nodes have the ability to authenticate and authorize appropriate information to satisfy 1996 Health Insurance Portability and Accountability Act (HIPAA).
- The nodes serve multicast communication for enabling data availability to multiple receivers
- Multiple routes are a necessity due to the mobility of both sender and receiver.
- Half-duplex communication is assumed between nodes
- Not all nodes in the network are compromised (i.e., k nodes out of N sensors)
- The source and sink node are unaffected by any DoS attack (i.e., relay nodes act as malicious nodes)
- Data transmission is strictly based on priority
- Every received message has a 't' delay, but less than a threshold to satisfy 'data freshness'.

3.3.1.1 Experimental Network

A network of 25 sensor nodes, the agents are spread at random across the network to speed up the search process. Monte Carlo simulations were performed for sensor node scattered across a 2D space with Euclidean distances between 2 nodes of

$$D_{12} = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{EQ 7}$$

The energy and threshold at each sensor node is varied, thus increasing the network's lifetime. The sensor's lifetime can be calculated using the modified definition of [59]

$$E(l) = \frac{\varepsilon_0 + \mathrm{E}(E_w)}{P_c + \lambda.\mathrm{E}(E_r) + \xi.\mathrm{E}(E_s)} \qquad \text{(EQ 8)}$$

where ε_0 is the non-rechargeable initial energy, $\mathrm{E(E_w)}$, expected wasted energy, $\mathrm{P_c}$, the constant power consumption, λ, the number of received messages, $\mathrm{E(E_r)}$, the expected reporting energy, ζ the sensing rate, and $\mathrm{E(E_s)}$, the expected sensing energy.

The agents are energy aware and know the energy status of each sensor node. As the agent moves from node to node, energy is lost through communication. The agents do not traverse nodes with depleted energy. New paths are set up that avoid such nodes so that communication remains functional without the degraded sensor. The agents do not require initial solutions in the system during initial setup. This allows the system to be more flexible, robust, decentralized and intelligent. These agents ensure the optimal route to the destination using limited resources and also learn the network environment. Initial computational cost and time is high but this drops drastically once the agents adapt to the network and environment.

The concept of sensor based health-care application is that nodes participate in routing if their energy is above a certain threshold. The sensor's whose energy fall below a set threshold is considered down or depleted. Thus, these nodes are neglected and an alternate route is taken. This keeps the network functional even during individual node failure. Only for a priority message, sensors with low energy levels participate in routing.

The agents accumulate pheromones as they traverse from source i to sink j. Hence distance travelled, energy, BER and hops are the critical parameters that need to be considered while depositing the trails. Hence (1) is modified for this cognitive protocol as

$$\psi_{ij}(t) = \rho\psi_{ij}(t-1) + \frac{Q.E_t}{D_t.H_t.BER_t} \tag{EQ 9}$$

where D_t, H_t, E_t and BER_t are the total distance, hop, energy and bit error rate performance, respectively, of the current agent in a tour. The link cost function is modified based on the QoS parameters as

$$\eta_{ij}(t) = \min\{[W_1.(\frac{H_a - H_r}{H_a})] + [W_2.(\frac{D_a - D_r}{D_a})] + [W_3.(\frac{E_a - E_r}{E_a})] + [W_4.(\frac{BER_a - BER_r}{BER_a})]\} \tag{EQ 10}$$

In (9) ‘a’ is the actual and ‘r’ is the required value for data transmitting. The minimization cost function for the normalized value of performance parameters is applied. Thus increasing the QoS and also incorporating the cross-layered meta-heuristic approach.

The transition probability for normal traffic determines the routes chosen by the ants and is calculated as in (2) using values from both (9) and (10). Whereas for handling priority events and random queries (distress signals), the priority of the message needs to be incorporated into the transition probability as

$$P_{ij} = \frac{(\psi_{ij}(t).\Gamma_{ij}(t))^{\alpha}.(\eta_{ij}(t))^{\beta}}{\sum_k (\psi_{ik}(t))^{\alpha}.(\eta_{ik}(t))^{\beta}} \tag{EQ 11}$$

where Γ is the message priority, and η is the global performance from the swarm agents

As previously discussed, the tabu-list is a main feature of the ACO algorithm, which keeps track of the nodes visited by the agents. In our C2SP algorithm, since we modified the pheromone and transition probability, the routes reflect energy efficiency and resource optimized solutions. The meta-heuristic algorithm ensures the optimal route to the destination using limited resources and also learning the network environment**.**

3.3.1.2 Simulated Attack Scenario

Interception of the secure information by enemy is an act that cannot be neglected. Hence, apt security measures need to be taken at every layer of a protocol design. The DoS attack is caused by the malicious node or a friendly node under adversary attack.

The main DoS attack imposed on the health-care is Wormhole, as they are simple passive attacks, i.e., attack is launched only if the malicious node receives a message. In a wormhole attack the 'malicious' node receives message from one end of the network and tunnel on the other using wired or wireless links. A act of tunneling the packets with low latency can gain neighbors trust as "shortest" route to destination. And also refrain the destination node from knowing multiple routes.

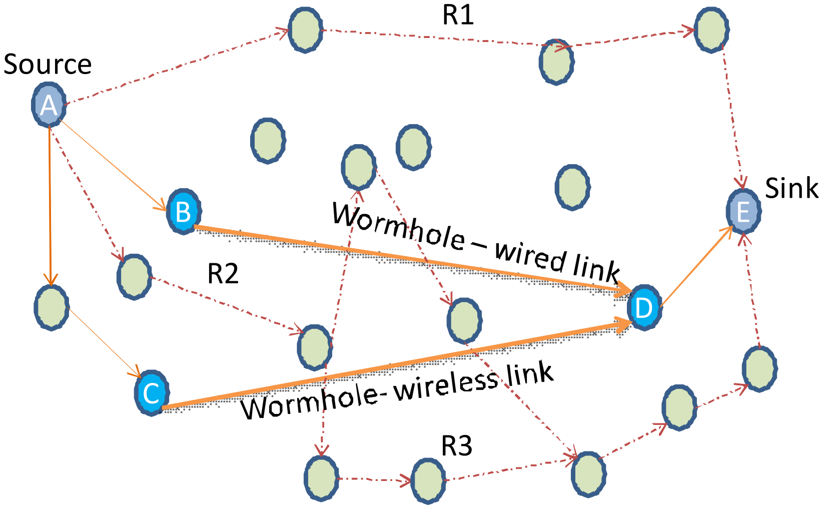


Figure 3.4. Wormhole attack on Sensor based Network

Figure 3.4 illustrates a wormhole attack, where nodes B and C are the malicious nodes with wired and wireless links directly to node D, and thus are closer to the sink (destination). Therefore, other routes R1, R2 and R3 is not discovered by the sink, and even if it was they get neglected considering the high latency. Many protocols such as Distance Source Routing (DSR) get trapped in such situations or application scenarios.

In C2SP, DoS attack is detected based on the updated tabu-list available to all agents. Since, the list maintains the distance, energy, number of hops, packet delivery and bit error rate of every optimal route taken, a random validation between the current route and listed path is matched for any distance or energy variation from the threshold. If the error falls within a expected threshold, the nodes along the route is assumed to be legitimate otherwise the entire route is penalized for a time instant t seconds. Since the tabu-list consist of back-up routes the neighboring node takes the next best optimal route from the list as an act of countermeasure. In health-care the nodes that join the network usually sends out a request for authentication, which can be used to our benefit as “probe” signal to check for wormhole nodes. Also, by knowing the wormhole locations, during emergency situations these wormhole nodes can be used as relay nodes. As the main objective is to diffuse data to the destination to save lives, while trading security.

3.3.1.3 Simulated Results

The simulation is performed on an Indoor and Outdoor health-care monitoring system under wormhole attack using Matlab. The message is communicated using Binary Phased Shift Keying (BPSK) modulation schemes, therefore the BER, energy consumption and packet delivery rate (PDR) in each of these cases are compared to verify, which attack worsens the performance of the application. The dependency of successful packet delivery, packet lost at the source, energy consumption, distance taken in reaching the destination and the number of hops is based on the weights assigned by human or artificial intelligence.

Table 3.1. Performance of Indoor & Outdoor Health-care Monitoring Against Wormhole attack Using C2SP

Node	PDR: Indoor	PDR: Outdoor	Avg. EC: Indoor.	Avg. EC: Outdoor.
2	0.9941	0.9953	18.3326	6.1957
4	0.9905	0.9641	15.0853	21.0754
8	0.8952	0.8326	32.7419	28.5675
10	0.7952	0.7167	76.0974	63.8761
15	0.682	0.6011	53.08	76.0887

In Table 3.1 the wormhole attack on an Indoor and outdoor application using C2SP is shown, where 2, 4, 8, 10 and 15 nodes are compromised. The robustness and resource efficiency of the application is maintained by C2SP with an average PDR of 87% and 81% for Indoor and outdoor scenario. The main objective of detecting the DoS attack is to increase the lifetime and reliability of the application, hence the average energy consumed and PDR is compared for an indoor and outdoor application. The threshold settings for both the indoor and outdoor were the same, which can be varied considering the influences of environmental conditions.

The key reason for choosing PDR and energy consumption is to balance the metrics optimally where maximization of PDR and minimization of energy is required. But under adverse conditions i.e., where a life of an individual is given higher prioritization, weight using POSETs is given to the PDR higher than the energy consumed.

3.3.2 Emergency Responder Network

In Figure 3.5 an emergency responder application [59] is illustrated where the rescue mission is carried out by installing an ad-hoc sensor network on the fly in real-time. QoS and response time to transmit information to the sink is critical. The sensors are placed by responders as they enter the building, and serve as bread crumbs from the source to sink. The sensors can be placed on the ground or mounted on the wall depending on the coverage needs. The data communications between responders and the command center can contain critical information. Hence, multi-user interference (MUI) needs to be reduced for the critical communications.

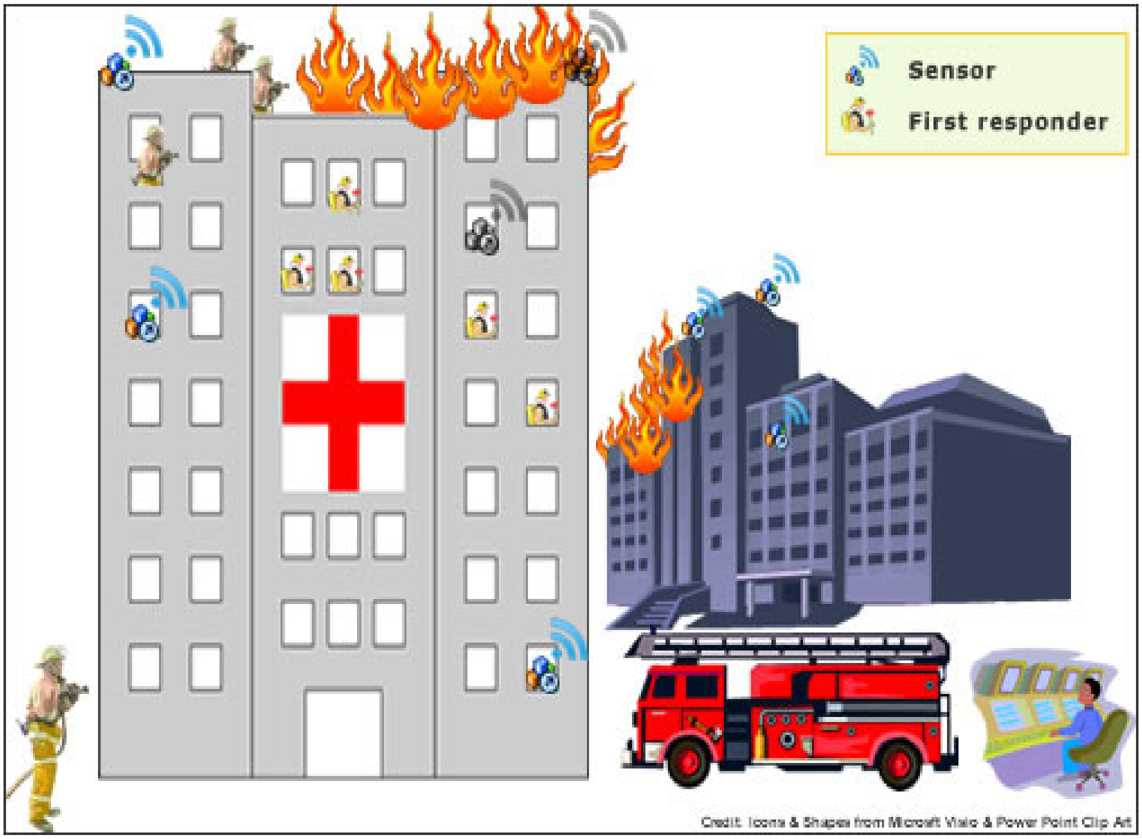

Sensor
First responder
Credit: Icons & Shapes from Microsoft Visio & Power Point Clip Art

Figure 3.5. Sensor based Emergency Response Network

The data routed from each responder to the sink (or command center) utilizes the sensors to relay messages in an optimal fashion. Several issues need to be addressed while designing a protocol for it. First, the data transmission such as voice, vital statistics of responders and victims from bio-sensors, and location of people and resources requires a protocol that can adapt to the needs of the emergency. Second, the distress signal by any responder should be given highest priority during routing. Third, the location measurements require time synchronization between sensors to minimize error and timely transfer to the command center. Apart from data transmission, the protocol should be robust and adaptive to incorporate sensor failures or additions.

In this application the primary target is to acquire location information of responder accurately, hence modulation scheme that aids in reduced error is best suited. There are many modulation schemes available for signal design. Instead of using carrier frequencies, ultra-wideband (UWB) systems transmit information using trains of short time duration pulses that spread the energy from the near direct current to a few gigahertz. UWB technology performs efficiently for two extremes in wireless communication systems: short range, high data-rate personal area network (PAN) applications such as the IEEE 802.15.3a at 3.1 - 10.6GHz and 802.15.4a longer range, low data rate personal area networks (PAN) applications below 960 MHz. A blueprint of the indoor building system is available at the command center, yet due to fire access changes constantly.

3.3.2.1 Experimental Network

In this application, we have designed two UWB pulses that can be considered orthogonal due to their frequency separation. The low data rate signal can be used for dual purpose, such as supporting data transmission for vital statistics and location estimates if time synchronization is carefully maintained. As one of the IEEE 802.15.4a physical layer technique candidates, Impulse-based UWB (I-UWB) is particularly attractive for sensor networks due to its resilience to multipath interference, simple transceiver circuitry, accurate ranging ability, inherent security, and low transmission power.

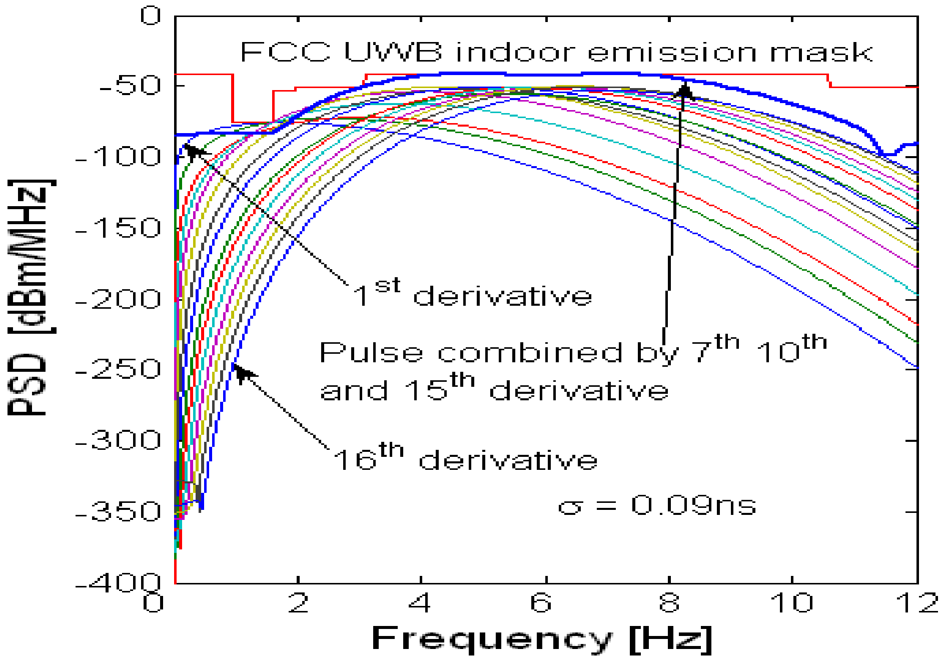


Figure 3.6. Power Spectral Density (PSD) of pulse combined by 7th, 10th and 15th Gaussian derivatives based on FCC Indoor UWB emission mask

The bi-pulse modulation in UWB is a special case of PAM modulation. We use one pulse with two polarizations. The peak of the pulse facing up stands for bit “1”, while facing down stands for “0”. The bi-pulse UWB can provide high data rates to neighboring sensor nodes when the network’s throughput is the critical function as well as a lower bandwidth pulse for low data rate messages [60]. When only sensing is needed, then UWB can support longer range measurements with slightly longer pulse lengths using the low bandwidth UWB pulse better suited for accurate time measurements. In order to transmit

UWB with other types of signals without interfering, without exceeding the power is a key design issue

One approach to resolve the key design issue is to combine different orders of Gaussian derivative pulses, the current most popular family of UWB pulses. An interesting feature of the Gaussian derivative pulse is that it naturally increases its "center" in frequency as the order of derivative increases. We take advantage of this and combine pulses as shown in Figure 3.6, the PSD of the pulses show that the designed pulse [63] not only conforms to the FCC indoor mask, but also effectively exploits the available power spectrum.

3.3.2.2 Simulated Attack Scenario

Due to the severity of location information in emergency responder application, the effect of Sybil attack is analyzed. In Sybil attack, the "malicious" node impersonates and becomes a part of multiple routes by denying genuine relay nodes from participating in routing. In addition, a Sybil node tends to relay messages initially and later drops the packets thus degrading overall application performance.

Figure 3.7 illustrates an example of Sybil impersonator [61] as node 'A', 'B' and 'C'. There are many approaches as discussed in Chapter 1 to reduce Sybil attack such as authenticating techniques. Since emergency responder uses nodes to identify their location on the fly, the first node placed acts as a beacon. The assumptions made on the simulated scenario is as follows,

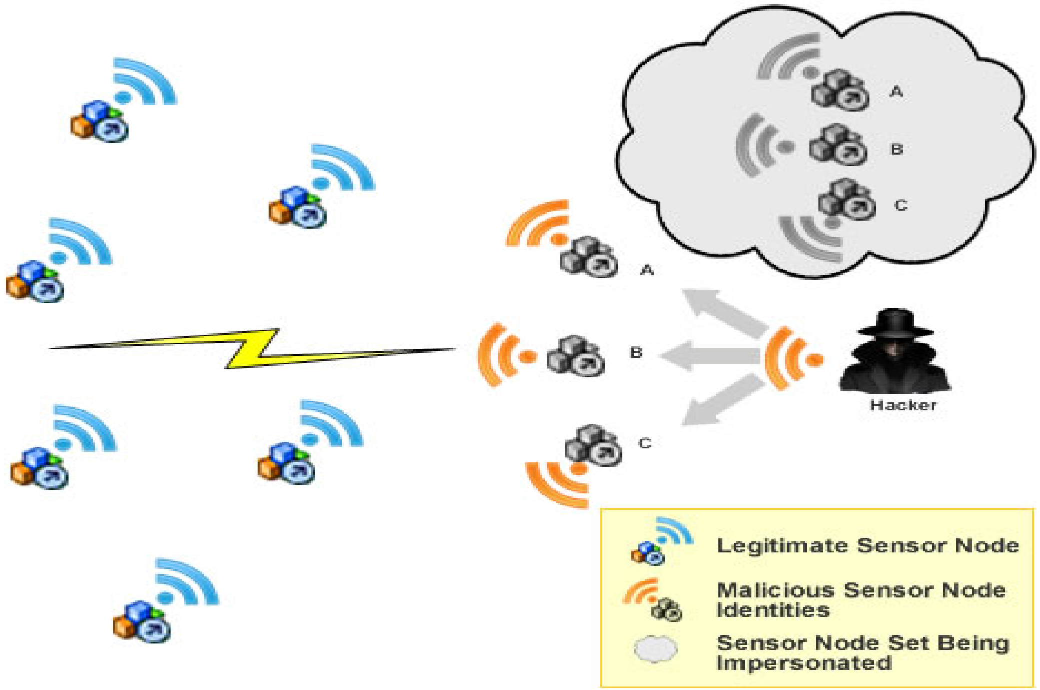

A
B
C
A
B
C
Hacker
Legitimate Sensor Node
Malicious Sensor Node Identities
Sensor Node Set Being Impersonated

Figure 3.7. Sybil attack in Sensor Network

- Only attacker has multiple identities, i.e., genuine node is always unique.
- Reputation/Voting of node is earned through ‘genuine’ neighbor trust.
- No two Sybil nodes are neighbors i.e., direct communication between ‘genuine’ and ‘fake’ nodes.
- Sybil nodes resource computation is inconsistent i.e., inefficient resource usage.
- Sybil node may drop or corrupt a message with ‘t+1’ delay.

In emergency responder application, there are multiple sensors that provide location information i.e., responder’s vital signal and radio. Thus, fusing different values can locate the impersonator accurately under severe conditions. During normal activity, only limited information is available and such impersonation leads to failure of packets being delivered to the destination and unnecessary exhaustion of resources by other nodes. Hence, predicting such an attack is crucial to the performance of the network.

3.3.2.3 Simulated Results

A sensor network with 25 nodes is simulated using Matlab, and equal number of agents randomly placed on the nodes. After converging, the agents adapt to the network using the knowledge acquired from their neighbors. The parameters settings of C2SP is from [62], and is assumed to be $\alpha = 4$, $\beta = 7$, $\rho = .7$, $Q = 9$. The initial pheromone value ψ as 10. The stability of the algorithm is analyzed by iterating all scenarios for 100 runs.

The robustness of the algorithm is analyzed in a noisy and fading channel using UWB Scholtz model [63] for pulse amplitude modulation (PAM) and pulse position modulation (PPM). The number of multiuser is assumed to be 6 for a resolvable communication path of L=2 and 4. The network's average BER, lifetime (energy) and PDR for low, medium (med) and high priority messages using UWB-PAM gives more data capacity in comparison to UWB-PPM when L=4. The message with higher priority is transmitted with more energy using power control schemes, whereas medium and low priority messages are based on normal traffic and thus give a prolonged network lifetime.

Table 3.2 shows Sybil attack on an indoor emergency responder system, and as discussed earlier, the malicious node corrupts or drops messages. Therefore PDR, BER and energy are given higher weights to identify the attack.

Table 3.2. Performance of Indoor Emergency Responder Against Sybil attack Using C2SP

No. of Sybil Nodes	PDR	BER (bit/s)	E (mJ)	Latency (sec)
2	0.96	0.0125	13.65	2
4	0.921	0.031	22.733	4
8	0.842	0.0424	21.229	12
12	0.75	0.066	32.345	13
15	0.6213	0.0829	41.507	19

3. 4 Research Conclusion

In this chapter the versatility and robustness of C2SP was analyzed using health-care and emergency responder application. C2SP performed reliably with efficient transmission during both Sybil and Wormhole attacks where half the network was under attack.

In the health-care application, C2SP’s random validation ensures longevity of routes and resources. If more than half nodes are compromised then this validation method may lead to penalizing routes with genuine nodes. Hence, there are limitations in using the threshold based approach, where only k nodes out of n nodes can be compromised. Unfortunately, when the source or the destination itself is under attack then the message is either stored at the neighboring node for a random time slot.

The PDR of wormhole attack on a Outdoor network was worse when compared with an Indoor scenario. This is attributed to the fact that outdoor environmental conditions such as fading, shadowing influence the performance of the sensors and the routing algorithm. The cognitive algorithm should consider these external conditions and therefore, should eliminate the presence of any intruder node. Simulation shows that wireless application is efficient in energy consumption while maintaining transmission accuracy. This also shows that the wireless health monitoring application is competitive to the traditional system in accuracy but not in terms of security. When wireless applications are considered security of application needs to be traded-off to a limited extent.

In emergency responder application, performance metrics such as PDR, distance, energy usage, and response time is weighted more than sensor’s lifetime. This is due to the assumption that lives are at risk at every time interval so the responders must be protected before the sensors. The parameters selection criteria is primarily dependent on the application, which can be modified as needed. UWB can inherently support multiple capacities while being naturally orthogonal. This characteristic with the C2SP controlling the communication layers can improve resource efficiency, adds robustness, operates in a de-centralized manner and adds flexibility to the message content and speed.

C2SP aids in routing messages through genuine nodes as a countermeasure whereas identifying and locating an attacker is performed more accurately using mining techniques that are discussed in the next chapter.

CHAPTER FOUR

Bayesian based C2SP Approach

"First act of security is to defend and then confront based on your resource availability"

In the previous chapter, a countermeasure was proposed upon detecting a security threat. As sensor nodes are prone to DoS attacks and detecting the threats is crucial in any application. This chapter is dedicated to accurately locating the malicious node when a threat is detected using characteristics learned about the application and environment. The C2SP approach uses POSets to weigh on performance metrics. This approach can be further improved using Bayesian intelligence in locating malicious nodes. In addition, an abnormal behavior of a node can also be predicted well in advance based on the availability of resource and training data.

Bayesian Networks (BN) is used in representing and reasoning problems by modeling the elements of uncertainty. The decision from the BN is applied to C2SP forming an hybrid intelligence approach to re-route the information and disconnecting the malicious nodes in future routes is discussed below.

4. 1 Bayesian Network

Bayesian Networks are used in representing reasoning problems by modeling the elements of uncertainty. BN algorithms can be used as a scalable approach to operational decisions such as prediction and detection concerning the sensor network. The algorithm of BN is applied to make decisions in the real world environment. BNs are constructed to represent the uncertainties that are interpreted by conditional probabilities during the process of situation assessment.

BN is a graphical model that represents probabilistically relationships among variables of interest. Let ***X***={*X1, X2,..., Xn*} denote a set of random variables related probabilistically through P(*X1, X2,..., Xn*), and *x1, x2,... xn* be the possible values taken by these variables respectively. BN consists of a directed acyclic graph (DAG) that corresponds to the conditional independence for ***X*** and the local aprior probability distributions associated with each variable. This structure gives the joint probability distribution for ***X***. The process for obtaining DAG can be implemented step by step. It starts by designating X_1, which means it is not influenced by any other variables, and assign it the aprior probability $P(X_1)$. Next if X_1 is a cause for X_2, then establish a directed edge from X_1 to X_2 and quantify this link with the conditional probability $P(X_2|X_1)$. X_1 is a parent node of X_2. If X_1 has no influence on X_2, they are conditionally independent and $P(X_2|X_1)=0$. At the *i*th stage, the node *Xi* has potential parents $\Pi_i \subseteq \{X_1, X_2, \ldots X_{i-1}\}$ represented by drawing the appropriate parent to child link with corresponding conditional probability $P\langle X_i|\Pi_i\rangle$. This hierarchical process continues until all variables have a place in the DAG and all causal relationships between parents and children are shown by direct links in the graph. The network formalism then provides the joint probability distribution for ***X*** given by

$$. \quad P(X_1, X_2, \ldots X_{i-1}) = \prod_{i=1}^{n} P\langle X_i | \Pi_i \rangle \qquad \text{(EQ 1)}$$

These joint probabilities then provide quantitative assessments of the problem domain that has been modelled. BN is used to maintain the relationships between desired performance values and parameter requirements for the system. Any scheme best works only if the application and its requirements are known. In this chapter, the jamming attack is analyzed to determine the location of the intruder. The characteristics of different types of jammer has varied effects on the network performance, which is discussed in the following section.

4. 2 Jammer Attack or Radio Interference

A radio interference is caused by using a jammer, which is a device that can partially or entirely disrupt a node's signal, by increasing its PSD. Jammer can never re-produce a signal nor can it pretend like a receiver node. A jammer intentionally reduces the QoS and increases transmission delay of the application. The application of spread spectrum (SS) techniques developed by the end of World War II. Using SS technique the data is spread across the frequency spectrum making the signal resilient to jamming, noise and eavesdropping. Depending on the modulation scheme opted for the physical layer, jamming the node from its peers varies.

4.2.1 Jammer's Characteristics

A jammer's sole purpose is to disrupt node's service but also to be coy of its existence. The parameters such as signal strength of a jammer, the location and the type influences the performance of the network and each jammer has different effect on the node.

There are different types of SS such as Direct Sequence (DS), Frequency hopping (FH), Time hopping (TH) and hybrid. There are advantages as well as disadvantages associated with using SS in sensor networks.

The advantages are as follows:

1. Ability to alleviate multi-path interference,
2. Jamming attacks reduced, and
3. Less power spectral density.

The disadvantages are as follows:

1. Bandwidth inefficiency,
2. Complex implementation, and
3. Computational cost.

Bluetooth [64]uses FHSS, which consumes more power as frequency hops needs to be synchronized. Whereas, Zigbee [65] uses IEEE802.15.4 standard where DSSS with CSMA-CA is used. Of late, Zigbee is being considered as the prevalent wireless technology for wireless sensor networks as it consumes less power. The modulation scheme for sensor network uses adaptive modulation technique in a Rayleigh fading channel. Thus, jamming this network that uses DS/FH spread spectrum is not trivial.

Figure 4.1 pictorially describes the jammer attack on a sensor network. The network is not only disrupted by adversary attacks but also by the environment. Differentiating the attack from natural environmental conditions requires knowledge of the various kinds of attacks that can be caused by an illegitimate user or intruder. Since an attack can completely eliminate a coverage area and in certain applications where network cannot be immediately updated, the network performance will be poor. Hence, study of different characteristics of an attack keeps the attack attempts at minimal as the knowledge of the types of jammers help in taking the appropriate countermeasure.

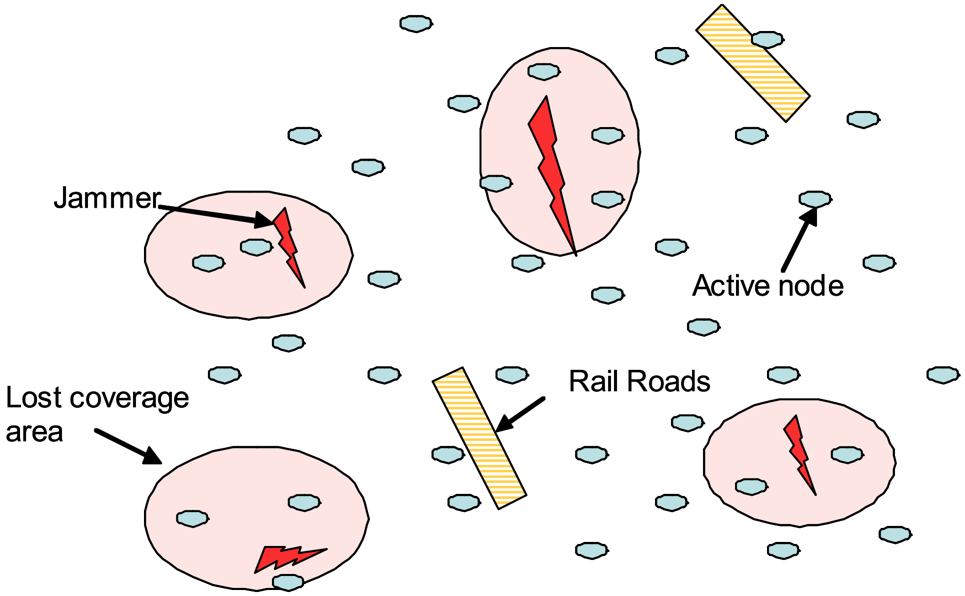


Figure 4.1. Jammer Attack on Sensor Network

In this chapter, it is assumed that there are four different types of jammers [66, 67, 68] namely:

1. Single-tone Jammer,
2. Multiple tone Jammer,
3. Pulsed-noise Jammer and
4. Reactive Jammer.

4.2.2 Single-Tone Jammer

A single-tone jammer (STJ) interrupts signal's whose frequency lies within the specified bandwidth of the signal and can be easily designed using an oscillator. A STJ targets any narrow band communication. Since traditional wireless sensor network use narrow band technology. This kind of jammer tries to continuously jam the node within specified bandwidth, which results in a dead link and diminishes the node's coverage. Recent sensor based applications consist of both existing modulation and wideband technology, jammers of all kinds should be considered while modelling a security scheme.

4.2.3 Multiple-Tone Jammer

A jammer that can disrupt the signal of some or entire channel (sub-carrier) of a multiple channel receiver. In this case, the attacker is assumed to have knowledge of the 'sub-carrier' of the node's spectrum. This type of jamming leads to a complete node failure when the entire channel is compromised. The only time the node can recover is when the jammer is turned off. Typically, an intruder plays it safe while jamming a node by occasionally turning off its radio. Thus, make the neighboring node assume the node is not under attack but rather lost its energy and needs recuperation. Hence, detecting a jammed node is very critical.

4.2.4 Pulsed-Noise Jammer

A pulsed-noise jammer (PNJ) is a wideband jamming, which behaves like a pulsed signal by turning on and off periodically. The primary goal of this jammer, is to disrupt the spread spectrum communication by spreading the peak jamming power during the "on" time. Two types of pulsed-noise jammers are considered, namely, slowly switching and fast switching jammers.

In slow switching jammer, the frequency of the jamming signal switching from “on” to “off” pulse is less than bit frequency of the genuine signal. Therefore, leading to jamming a signal for a whole symbol duration Ts. Therefore, a genuine transmission signal loss is encountered, yet the BER or the number of corrupted messages are less.

Whereas in a fast switching jammer, the frequency of the jamming signal switches from “on” pulse for a fraction of symbol duration Ts, and remain “off” for the rest of the signal. Thus affecting the ‘genuine’ signal and corrupting message transmission.

4.2.5 Reactive Jammer

Reactive jammer is one of the worst jammer attack, as it would cripple the node of its service by being active anytime it senses the node’s availability. Although this strategy of constantly jamming the node’s service leads to easily identifying the existence and location of jammer, yet it achieves its purpose of degrading the application’s performance. An intelligent jammer attacks nodes such that both neighboring nodes and the victim believes there are no relay nodes forcing them to go to idle to sleep mode.

In the following section, mathematical formulation based on the different types of jamming is described with simulations.

4. 3 Bayesian based C2SP

Bayesian based information depends entirely on the node’s attributes by monitoring a group behavior over a period of time. Detection of any attack is important while trying to secure the link from intruders. Hence a hypothesis is formulated that helps in detecting whether the DoS claim is authentic.

The jamming attack can be classified into four possible decisions namely,

1. Sensor out of resources - is accepted,

2. Sensor encounters a resource outage but falsely calls it a Jammer attack,

3. DoS-Jammer attack is accepted. and

4. DoS-Jammer attack is rejected and claimed as resource outage.

The accuracy of the decision is specified in terms of the rate with which the system makes decision 2 and 3, which are erroneous. The error described in 2 is referred to as False Rejection Rate (FRR). The error in 3 is the False Acceptance Rate (FAR). Genuine acceptance rate (GAR) is one other performance measure, where GAR = 1-FAR. These quantities are specified in terms of conditional probabilities. In detection theory [ref-69 final], FAR, FRR and GAR are commonly known as the false alarm rate, miss rate and detection rate.

The problem of DoS using jamming attack in the physical layer of a sensor network can be formulated as a hypothesis testing problem where the two hypotheses are

H_0: The DoS claim is false and

H_1: The DoS claim is genuine.

The claims made by the BN directly reflects as weights on the route by penalizing nodes. This can be revisited upon verification of false claims. There is always a possibility of false positives and false negatives based on the severity of the environment and attack model.

The receiver operating characteristic (ROC) curve serves as a tool for analysis the false positive rate with the sensitivity of the application. Using the generic ROC curve as shown in Figure 4.2, the suboptimal solutions are discarded. As for our bayesian based C2SP approach, the detection rate of jammer attack and the false positive is considered a valuable resource in eliminating unwanted solutions and also in detecting the jammer's location. The location of the jammer is achieved by taking a centroid of all the DoS claims from the 'genuine' nodes. Although, the jammer location is obtained only after a few iterations or the purpose of eliminating it from future communication is more critical.

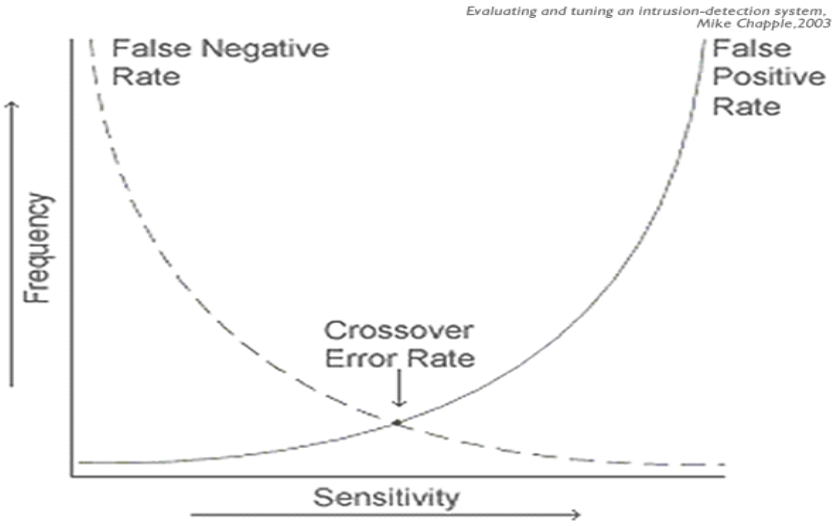


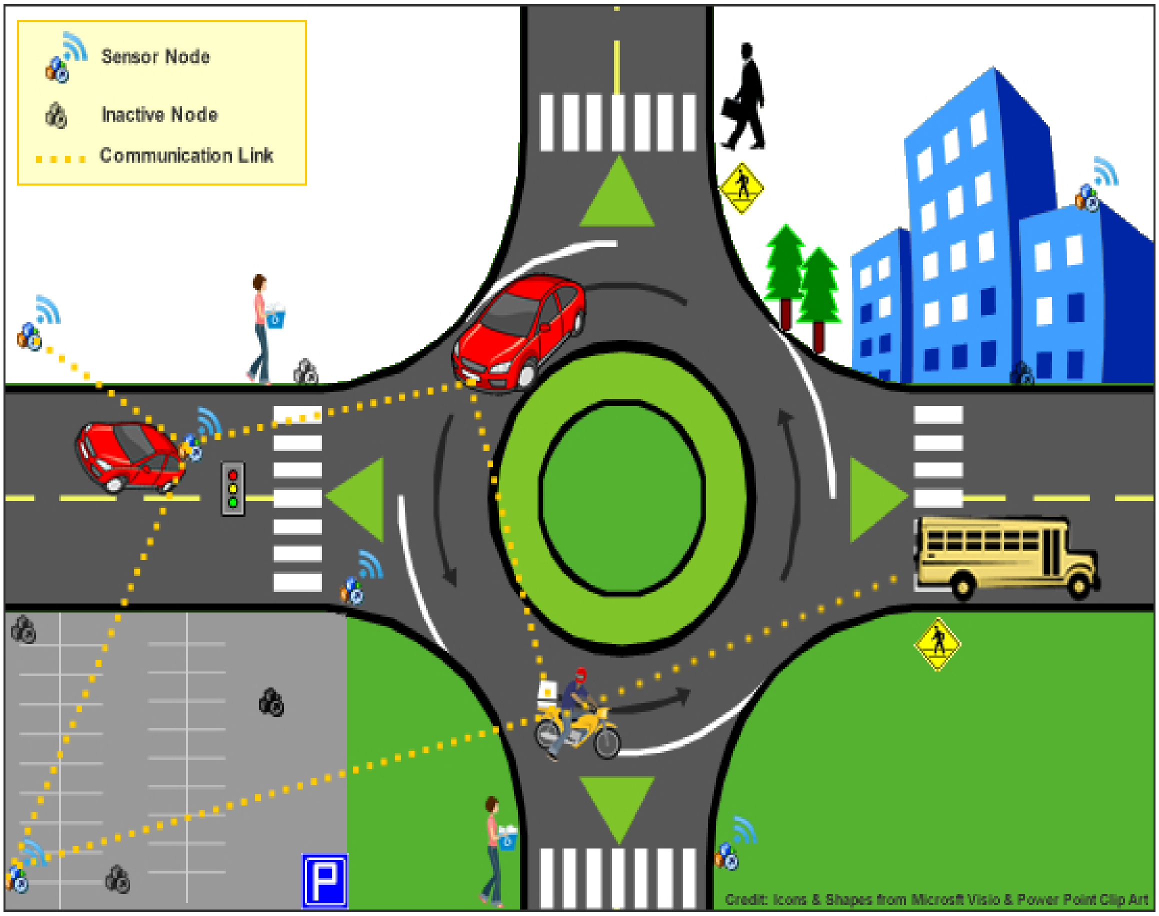
Figure 4.2. Denial of Service Detection

The BN resides at the 'super' node, which has infinite power and bandwidth thus enabling it to act as a watchdog and mine information received from multiple nodes. A jammer usually sends out a noise signal and hence a measurement of signal-to-interference -plus-noise ratio (SINR) is essential.

The performance of bayesian based C2SP approach against jammer attacks is tested on vehicular ad-hoc network scenario. In VANET application both narrowband and wideband technologies are used and the nodes adaptively communicate with neighbors and base station based on its functionality and availability. In the Biometric application only narrowband technology is used, where each node has prior knowledge of its location. Hence, varied types of jammer affects can be studied using simulated VANET and Biometric application.

4. 4 Vehicular Ad-hoc Network

A growing need for automated and intelligent transportation [52] support is required to facilitate dynamic on-road assistance, emergency evacuations, etc over a vast geographic area. Current transportation support system has many shortcomings such as mobility, scalability, adaptability and cost. Devices and applications based on wireless technology promises cheap and tiny sensors that can sense information within its coverage area and relay information using multi-hops.



Credit: Icons & Shapes from Microsft Visio & Power Point Clip Art

Figure 4.3. Vehicular Ad-hoc NETwork (VANET)

Vehicular Ad-hoc network (VANET) is an emerging technology where vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communicate in a wireless manner using dedicated short-range communication band. Figure 4.3 illustrates the system model of a cooperative, distributive and de-centralized VANET. In VANET issues like response time, data aging, bandwidth, packet delivery, message prioritization and communication cost is a major concern.

The sensors are embedded in the vehicles and surrounding transportation infrastructure. The node's state can vary based on its energy level and environmental conditions. A cooperative network benefits the users with different wireless technologies and QoS. The model shown below redirects the traffic to a parking lot using intelligent parking system feature. Thus a collaborative approach is advantageous in situation like emergency evacuation or traffic congestion.

The primary task of the VANET is to aggregate and facilitate information to and from all the neighboring vehicles for situation or threat assessment. Apart, from neighboring vehicular information, other data sources like passenger interest, radio, satellite, traffic management information can also be applied to improve the quality of information (QoI). Although, VANET promises to solve shortcomings of current technology, DoS such as jamming attack has become a major concern in these applications.

Data communications between sensors and base station (BS) is triggered by a query. These queries can be generated continuously, based on priority, time based or in an as needed basis. A continuous query is deterministic and is targeted towards data from a location or region of interest. During time sensitive or critical scenarios such as distress signals or accidents, an event is triggered and given higher priority to be queried to BS or nearby sensors to alert of oncoming traffic congestion or nearest healthcare facilities. Such events are non-deterministic and are classified as priority queries. Timely queries are made based on an individual's interest during any pre-set time. For example, during busy traffic hours and delays due to construction are obvious times when a critical message may need to break through the heavy communication traffic. The need-based queries are sent when any node or BS requires additional information for validation purposes. Upon sensing any event, nodes are triggered to collect, fuse, and relay the messages to the destination.

The sensor nodes are equipped with encryption techniques that ensures secure data packets, but the control packets are vulnerable. Hence there are some assumptions made in this application.

- Energy is not a concern in VANET
- Nodes are densely populated over the network
- Every node has the ability to store data of its interest for a time period 't'
- Data is communicated in discrete time frame, i.e., unusual speed, delay, etc

4.4.1 Experimental Network

A network with 25 nodes is considered in this simulation run with agents randomly placed on the nodes. Figure 4.4 provides a pictorial description of the algorithm used in VANET. The only input required by the agents are network parameters, the location of the sensor and initial parameters for the C2SP. The number of agents is proportional to the number of sensors in the network.

The network is built based on the following assumptions, such as,

1. All nodes are initialized with varied energy level, thus giving each different capacity to transmit messages.
2. Each node has varied threshold and their missions are varied.
3. The source and destination nodes are considered reliable.
4. Tolerance is set for every packet loss and successful packet delivery, beyond which, a node is penalized for it's behavior and
5. The probabilistic approach of the agent depends on the latency and the percentage of false decision. The two factors need to be minimal.

.

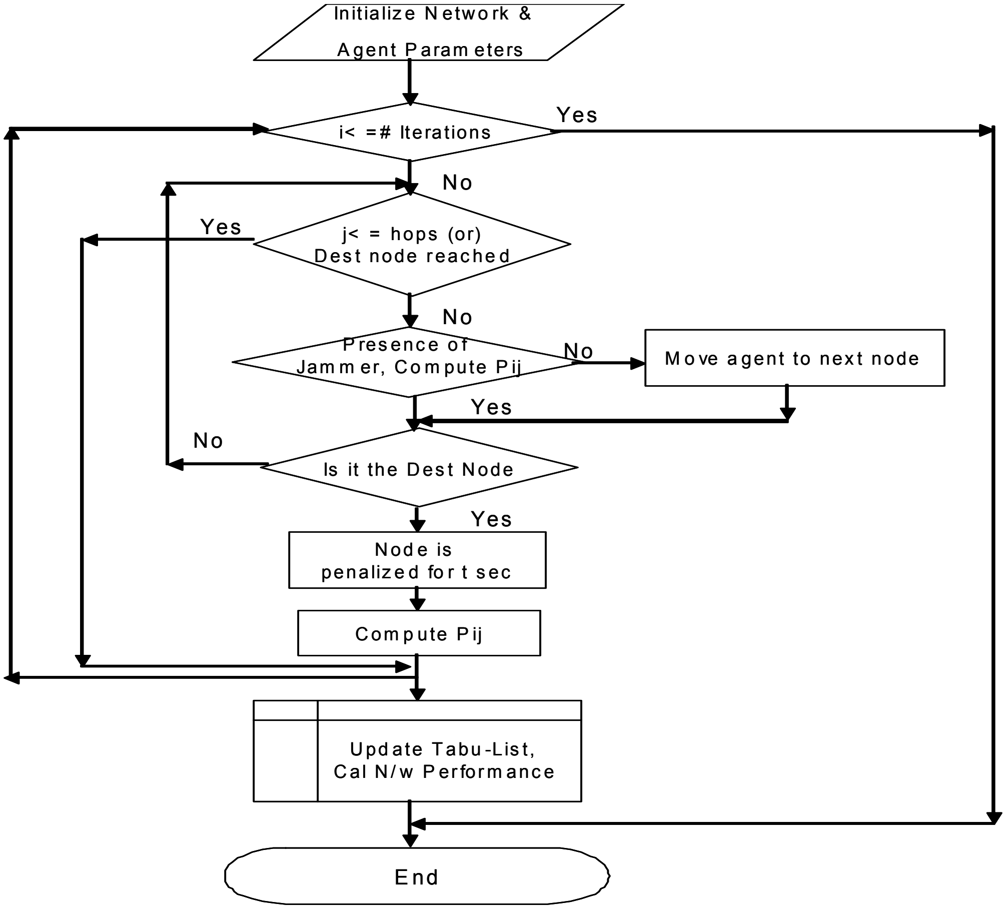


Figure 4.4. Flowchart - Detecting Jamming attack in VANET [70]

4.4.2 Simulated Attack Scenario

VANET is a densely deployed application, and hence jamming attack can be easily launched. Also, the network cost and size are very dynamic. Any signal can be jammed by a neighboring vehicle intentionally or unintentionally, but if the outcome leads to potential threat to application then even the genuine user will be penalized. Also, the transmitted message in VANET is encrypted and only packet size and timing can be manipulated by jammers.

Due to BN based knowledge, the factors such as BER, distance, latency, hops, node reputation, packet delivery are constantly analyzed against the historical (training) data set. The main advantage of VANET, is when multiple vehicles around the same vicinity are encountered with attack a prolonged data loss can also indicate abnormal behavior.

4.4.3 Simulated Results

The table below illustrates scenarios using different types of jammer and the effectiveness of evolutionary algorithm in assessing the performance of the network. The proposed detection and defense mechanism is simulated using Matlab. The performance of the network can be evaluated based on

1. Varying Jamming to signal ratio (J/S),
2. Energy to jamming density ratio,
3. energy to noise density ratio,
4. multi-path interference,

The parameters of ant system are assumed to be $\alpha = 4$, $\beta = 7$, $\rho= .7$, $Q = 9$ and initial pheromone value, y as 10. The source and destination nodes were assumed reliable. The stability of the algorithm is analyzed by iterating all scenarios for 100 runs. The actual hops is user defined which varies depending on the problem assigned. The normalized value of hops is given as H_{Norm}. The predicted distance helps in making a decision whether the nodes in the current route is still capable of communicating with its peers in the next iteration.

Figure 4.5 illustrates the BER for DSSS-BPSK model for image coefficients with with three different priority levels. The normalized BER for high priority coefficients is given by red circles, the normalized BER for the medium priority coefficients is denoted by yellow '+' and the normalized BER for the low priority coefficients is denoted by green '*' symbols respectively. The BER achieved for high priority coefficients is much less compared to messages of low priority coefficients. Using this analogy, a typical message transmission between nodes during normal behavior can be modeled.

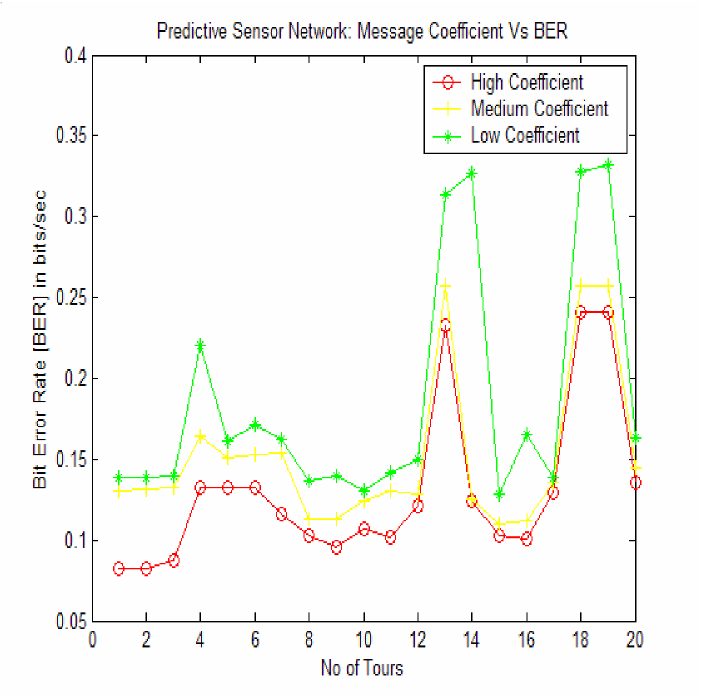


Figure 4.5. Message Prioritization of co-efficients in Sensor based Application [71]

Table 4.1 shows the performance of the network where single tone jammer is applied. Initially, the number of jammed node in a period t seconds is 3. Hence, the number of nodes jammed is 3 out of 25 in the network. Similarly in each case nodes are jammed for t seconds. Since single tone jammer affects only one carrier, and the modulation used here is DS/FH, therefore the probability of finding the PN sequence by the jammer is low. The performance of the network is based on the distance, latency and packet delivery.

Table 4.2 shows the performance of the network when multiple tone jammer is applied.

Table 4.1. Performance of Sensor Network -Single Tone Jammer

# node jammed	Average Distance	Average Latency (sec)	Average Packet Delivery
3	9.756	1	97.349
6	24.205	6	95.2798
9	35.3302	8	69.3568
12	92.373	12	78.7423

In this type of jammer, all the carrier is jammed in a single node if its under attack. The node recovers from the attack only after t seconds, so the chances of assuming the node has either left the vicinity or data freshness criterion is not achieved.

Table 4.2. Performance of Sensor Network -Multiple Tone Jammer

# node jammed	Average Distance	Average Latency (sec)	Average Packet Delivery
3	4.937	4	99.230
6	5.920	6	98.410
9	20.203	18	92.938
12	94.297	18	60.239

In Table 4.3 performance of the network when attacked by pulsed-noise jammer is shown. In this case, the number of nodes under attack did not affect the network's performance. As the duty cycle of this jammer increases it's signal strength only during the "on" duration. Since the DS/FH modulation rarely falls in the duty cycle, even when 12 nodes where under attack the network performance was fairly good. As shown, the pulsed-noise jammer does not influence the performance of the network.

Table 4.3. Performance of Sensor Network -Pulsed-Noise Jammer

# node jammed	Average Distance	Average Latency (sec)	Average Packet Delivery
3	1.202	7	99.008
6	2.45	13	99.129

# node jammed	Average Distance	Average Latency (sec)	Average Packet Delivery
9	8.2093	19	98.2108
12	28.2928	29	78.9812

Table 4.4 shows the network performance when reactive jamming attacks the network. Since reactive can disrupt the network based on the node's signal detection. This type of jammer affects the network performance very poorly. When 12 nodes are attacked by reactive jammer, the network performance is degraded, but the jammer detection is nearly 100%.

Table 4.4. Performance of Sensor Network -Reactive Jammer

# node jammed	Average Distance	Average Latency (sec)	Average Packet Delivery
3	10.2921	10	82.1823
6	17.185	20	73.976
9	40.4931	31	40.209
12	70.0383	35	0.0034

As shown above, the latency of the network is not affected by the presence of a STJ whereas reactive jammer easily reduces the performance of the application for both narrowband and wideband technology. Due to the increased latency the data freshness feature of the agents and system is affected and many node's reputation is penalized until the jammer's location is detected.

Finally, the most important feature of extending the learning feature of C2SP is to locate the adversary. Table 4.5 shows the detection rate of the proposed framework attained nearly 99% during reactive jammer attack but at the loss of application performance. Whereas, detecting a multi-tone or pulse-tone jammer is about 85% and above.

Table 4.5. Jamming attack detection Using Bayesian based C2SP Approach

Type of Jammer	Attack Scenario	Detection Rate (%)
Reactive Jammer	10%	79
	25%	83
	50%	99
Multi-tone Jammer	10%	67
	25%	77
	50%	95
Pulse Tone Jammer	10%	77
	25%	78
	50%	90
Single Tone Jammer	10%	74
	25%	80
	50%	85

4. 5 Biometric Building Access Network

This research was inspired by the need for a flexible and cost effective biometric security system. The flexibility of a wireless sensor network makes it a natural choice for data transmission. Unlike human intelligence based face recognition, the computerized face recognition using tiny inexpensive sensors with limited processing power and energy is a challenging task. 3D faces are usually represented by 2D gray scale images or 2D RGB color images. Whereas, the 2D facial images are affected by many factors such as lighting conditions, poses, facial expressions, and age[72]. The desired biometric recognition system should tolerate the intra-person variations while distinguishing the inter-person variations.

In temporarily enhanced security situations, a wireless constructed security system is more flexible and cost effective by designing a communication network that adapts to the environment and the sensors.

A temporary face recognition system (FRS) can be set up easily by placing a camera near the region of interest and transmitting the data through wireless channels to the processing center placed at convenience. Data that is either the full image or representative coefficients need to be transmitted with high fidelity to the remote processing center where the face recognition database is stored.

In [73], the robustness of wavelet transform to transmission loss is shown. Therefore, the data in transmission is preferred to be the wavelet coefficients rather than the original image. In this paper, the contourlet transform is experimentally shown to be able to further decrease the mean square error from the wavelet transform, and their performance is tabulated.

Figure 4.6 illustrates the routing of image coefficients to construct a robust face recognition by a wireless sensor network. The message is transmitted from the start node, denoted by a circle attached with a camera icon, to the destination node marked as "DataBase". The active sensor nodes are denoted by dotted orange circles and inactive nodes are denoted by blue circles with vertical stripes. The green lines show the actual route taken by the swarm agent. The dotted red lines show the alternative route that the agent could have taken. The agents travel through the route with less load, energy consumption, and transmission error. The selected route is evident to be shorter and more efficient. The data collected at the destination is processed and the acceptance or rejection decision is made.

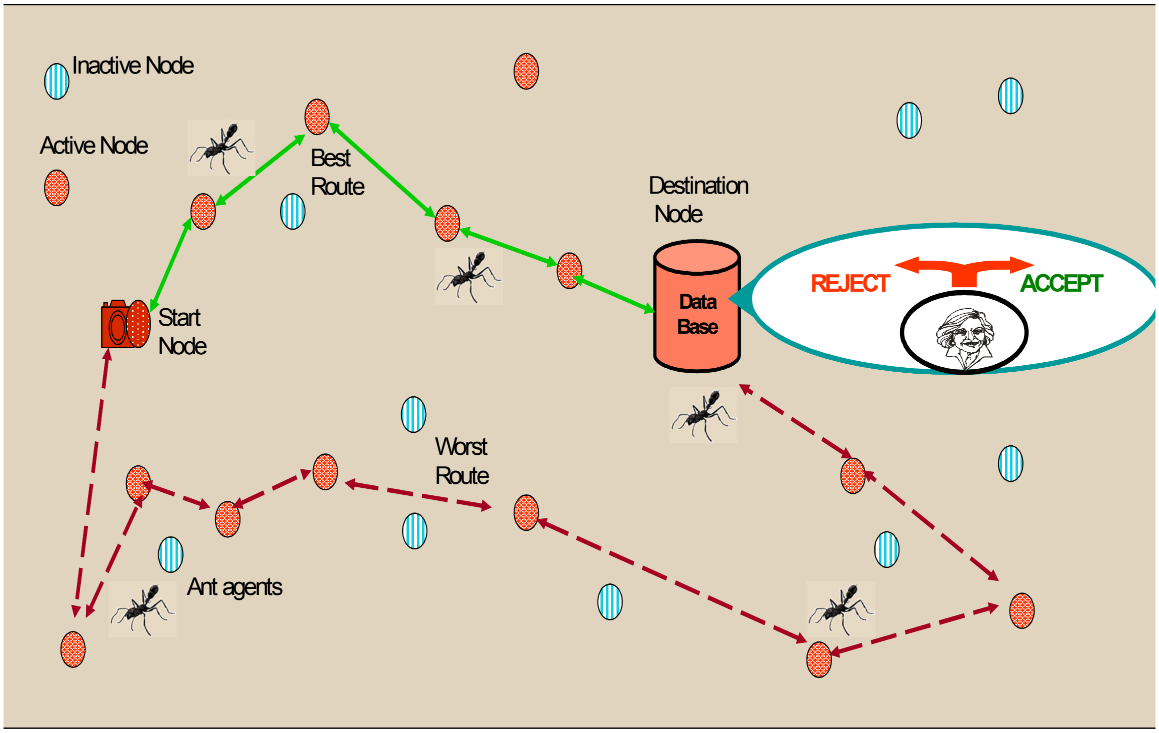


Figure 4.6. Routing Image Co-efficients in Sensor Network

Within the camera sensor near the region of interest there's a small chip for image compression and preliminary face tracking. The chip includes a small buffer to store the raw image in case a finer raw image is needed later on. By discrete wavelet transform or contourlet transform, a coarser image at a lower resolution can be produced to locate a face with less computation resources and to transmit the coarse face to the face recognition system with less bandwidth and energy. Once the face recognition system determines that there's a possible target, it will require the camera to send in the finer raw image and scrutinize it in more detail.

For data coding efficiency, the coarse scale image is derived by wavelet decomposition or contourlet transform. The coarser image is lossy by zeroing out the detailing coefficients. If all coefficients are used in reconstruction, the reconstructed image is lossless.

The bandwidth requirement increases from coarse scale to fine scale since the finer scale image needs more nonzero coefficients to represent it. The detailing coefficients are usually very small and dense near zero; entropy coding is very efficient in representing them. This improves the efficiency of transmitting the encoded coefficients describing the facial details as well. This kind of architecture increases the speed, and efficiency with reduced energy consumption and transmission error. In eigenface classification system, the basis vectors are stored in the destination node to compare with the reconstructed face based on received coefficients. If the transmission network can maintain the speed and efficiency of the system, then the face recognition system is robust in nature.

4.5.1 Experimental Network

In this application, the nodes use C2SP as their primary routing protocol and BN as the database to support multiple image registration and enhance personnel identification. There are 25 static wireless nodes, and 5 wired nodes, that participate in routing. The data transmission is carried only in the wireless medium. Although biometric systems can be a combination of image, voice, iris and fingerprinting, we primarily focus on face recognition aspect of the biometric system. Since, image co-efficients require additional transformation to deduce the information to co-efficients and hence computational and processing cost needs to be considered in the application and algorithm design.

Figure 4.7 illustrates the Bayesian network for detecting any types of DoS attack. The performance metrics and the sensor's characteristic is compared against to detect any anomaly behavior and upon detection of the attack, the bayesian sets the threshold on the parameter's settings. Hence, the constant update of threshold keeps the application adaptive based on the situation and mission of the application.

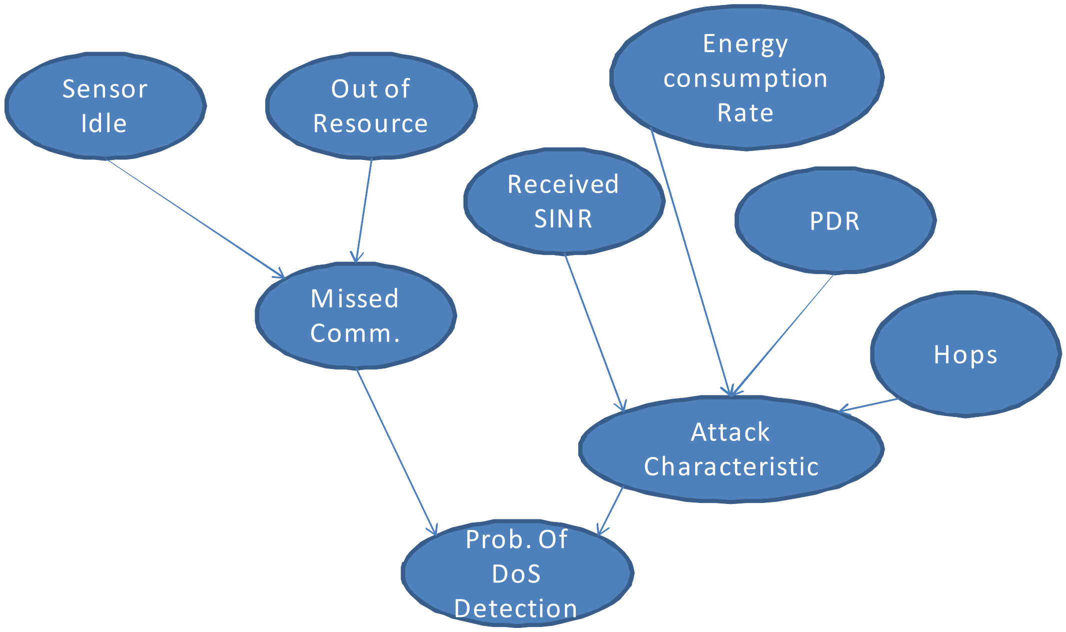


Figure 4.7. Bayesian Network for any DoS attack detection

4.5.2 Simulated Attack Scenario

In this chapter, we only simulated the jammer attack and hence, the VANET and Biometric application both have sensitive data and are similar in many ways, the assumptions of attack scenario is same in both cases. Except for biometric system, as its applied indoor environment, the influence of shadowing etc is removed in data transmission but the data itself undergoes high scrutiny due to the non-cooperative behavior of user's. Due to the availability of wired nodes with constant monitoring, a feedback on user's behavior can also be used as a feedback.

4.5.3 Simulated Results

Figure 4.8 and Figure 4.9 show the performance of the biometric application where low packet delivery rate of a node directly influences the % of correct acceptance and refusal of the user i.e., an intruder could be given access to the building and a genuine user could be deprived of his privileges, thus jeopardizing the application. Figure 4 and Figure 4.9 shows the impact of jammer attack on a biometric building access system. Thus an influence of a jammer attack is primarily based on the type of jammer, which can be avoided by knowing the characteristic and by predicting the attack.

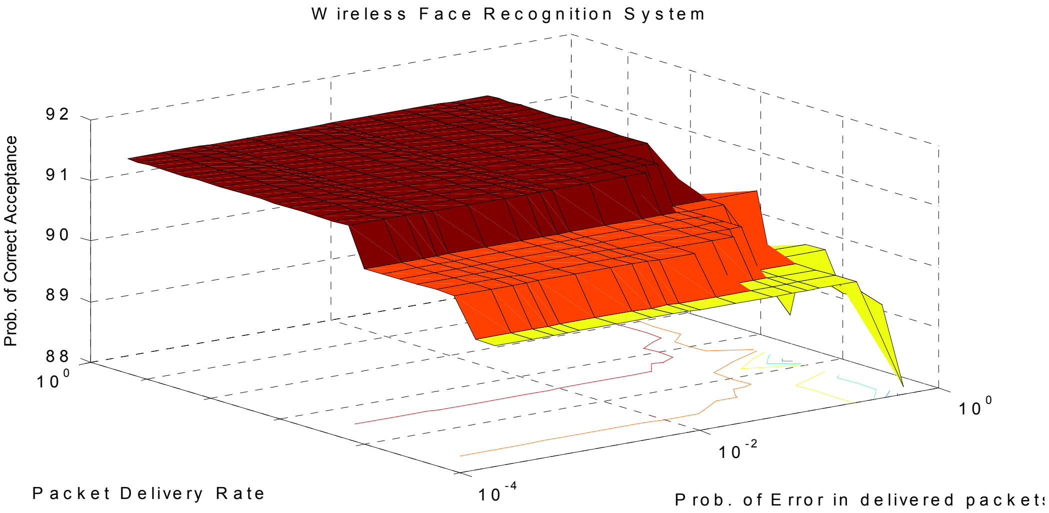


Figure 4.8. Performance of Biometric system wrt PDR Vs. Prob of Correct Acceptance.

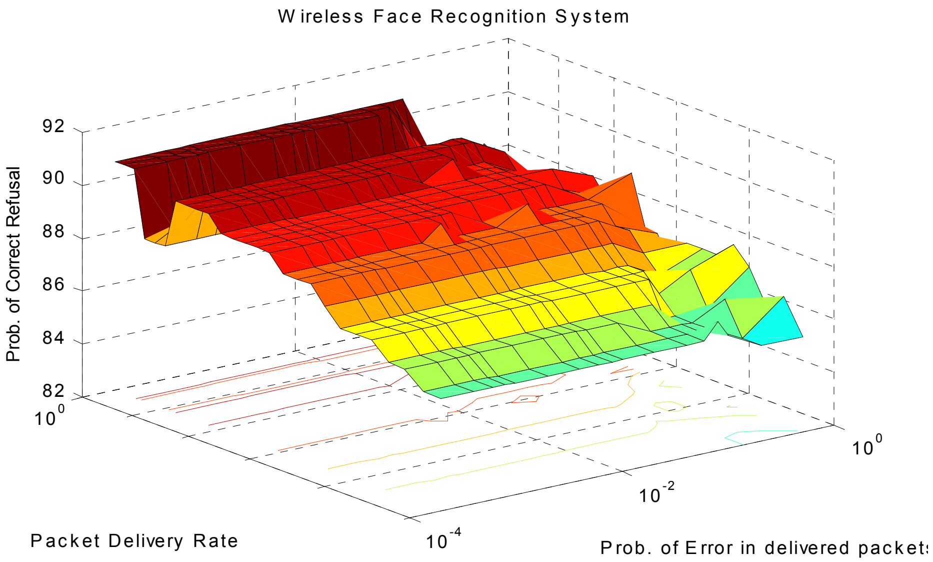


Figure 4.9. Performance of biometric application wrt PDR Vs. Prob. of correct refusal

Table 4.6 gives the simulation results of different jammer attacks, where 12 nodes are jammed out of 25 sensors in a network. The performance of the system is maintained under single tone jammer, multi-tone jammer and pulse-noise jammer attacks. The agents re-routes the messages and also with the help of the FHSS and DSSS techniques the signals are switched between channels. Unfortunately, a node under reactive jammer attack has no such options, as the entire channel is under attack by means of a high power noise signal spread along the spectrum. Thus for any application reactive jammer attack will degrade the performance, and the only way for the sensor nodes to avoid reducing their lifetime is by going to 'idle' mode.

Table 4.6. Performance of WSN against jammer attacks

Type of attack	**Energy Depleted**	**Average Packet Delivery Rate (PDR) (%)**
Single Tone Jammer	50.0292	78.7423
Multi-Tone Jammer	97.392	60.239

Table 4.6. Performance of WSN against jammer attacks

Type of attack	Energy Depleted	Average Packet Delivery Rate (PDR) (%)
Pulsed Noise Jammer	31.920	78.9812
Reactive Jammer	70.0383	0.0038

4. 6 Research Conclusion

The performance parameters such as hops, distance, packet loss, SNR, BER and packet delivery influences the decision taken in anti-jamming techniques. The network under 75% reactive jammer attack is shown to be functional indicating the robustness of the C2SP. The four scenarios presented in the result section re-emphasize the fact that a network remains functional and assesses the situation under all critical conditions. BN applied an adaptive knowledge in assessing the situation, and detecting an attack. The functionality of C2SP is to avoid jammed routes and find an effective countermeasure.

The data sensitivity of the VANET and Biometric application is protected by encryption algorithms. In addition, only vehicles that are registered for on-road assistance and smart-parking features can participate in message transmission. Hence, reducing the congestion and also avoiding unwanted traffic to unwilling users. Whereas, in biometric application, the sensitivity of the application requires users to be pre-registration of their biometric information.

CHAPTER
FIVE

Intrusion Detection System

"Security comes from learning not one's mistakes but from anticipating adversaries threat"

In the last chapter, a bayesian based learning technique was used to detect adversary or intruder's location during an attack. In this chapter, the art of learning from the intruder is explored. In recent years, Intrusion detection systems (IDS) have become widely popular in wired and wireless link with many promising solutions. In sensor based applications, there are many criterion that restricts the use of traditional IDS approaches. Hence, in this chapter the final phase of the framework, an intruders behavior is learnt to improve the robustness and security by exploring the use of a sensor network in a military application such as battlefield deployment.

5. 1 Intrusion Detection Framework

IDS is a process that was developed to ensure security of data and application by monitoring for anomalies and reporting to the base station. Most IDS are designed with signature-based techniques. The IDS is trained with data to learn the normal traffic flow and to differentiate regular traffic from an impending attack. There are two possible ways of protecting the network,

a) Intrusion detection (ID) framework and

b) Countermeasure upon detecting an attack.

There are many IDS and most of them are static, i.e., they can detect attacks using existing templates. Hence, any new attacks can be left undetected otherwise require frequent updates to keep application current. In addition, apriori modeled systems reduces false positive results, and accurate attacker claims can be obtained.

The primary features that makes any sensor based application successful are,

1. Secure and energy-efficient routing [17, 43]
2. Anomaly based detection
3. Improve accuracy of detection rate i.e., reduce false positive claims
4. Adaptive QoS features
5. Traffic Prioritization

There are different types of attackers, 1. Unintentional or amateur attacker 2. Knowledge of the application and 3. Expert knowledge of the application protocols, requirements, and architecture.

The primary concern of IDS is designing the models as templates for identifying malicious behavior. Also, there are numerous attacks that can evolve within a network i.e., insider and outsider attacks. The key feature of a successful IDS is not only to detect an intrusion but also to recover the node from the intruder attack.

5.1.1 Bait Architecture

The process of mimicking real-traffic to lead the adversary into gaining knowledge of the network is called ‘bait’. In our application, sensors that are idle during routing are termed as ‘bait’ nodes, i.e., upon detecting an anomaly the agents triggers these nodes to have virtual communication with the attacked node. This action of virtual communication, is dedicated to learn the intruder’s pattern. There are two types of ‘bait’,

1. Low interaction,
2. High interaction

Low interaction ‘bait’ only involves neighboring nodes monitor for any anomalies. In high interaction ‘bait’, a group of nodes with different coverage are used for predicting future attacks using pattern recognition. The initialization cost, resources and time are the two most important factors in determining the type of ‘bait’ for any application. The ‘bait’ nodes lures and acts as an accomplice to record intruder’s attack. Thus, learning from the intruder enhances countermeasures and defense mechanisms.

Figure 5.1 illustrates the implementation of ID framework. The network comprises of sensor with missions such as sensing, collecting, distributing information and acting as ‘bait’ nodes. When the information of the person or object of interest is flagged by the agents, the data is communicated to the destination (database) node, where the decision of whether its a normal activity (acceptance) or an intrusion (rejection) is made. Simultaneously, an intruder trying to gain access to the network is shown using 3 bold arrows. The intruder tries to communicate to his/her neighboring nodes which are active, but seldom does he know that his actions are been recorded and tracked at each ‘bait’ node using agents.

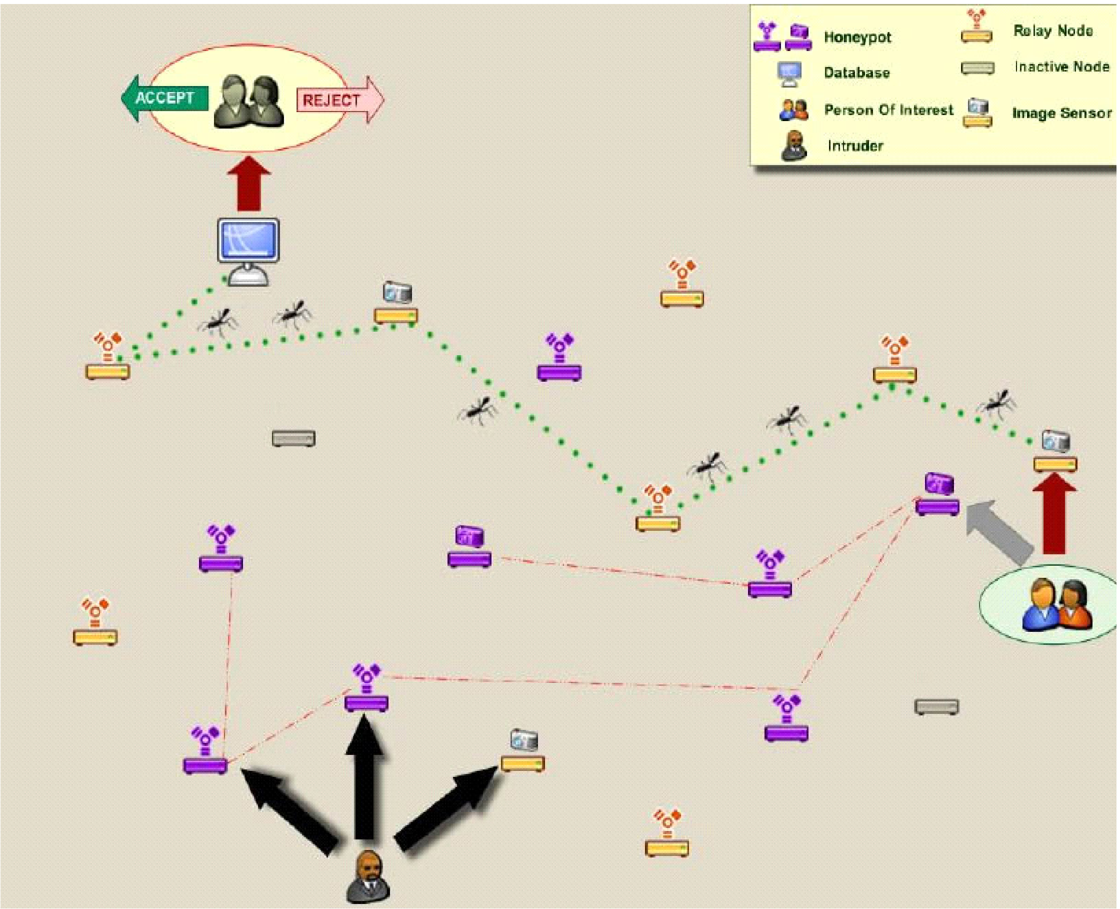


Figure 5.1. Framework implemented Using 'Bait' Architecture

The nature of agents sharing of local information with its neighbors can be strategically used to the user's advantage to trap the intruder using 'bait' trails. Since the 'bait' nodes should not receive any traffic from genuine nodes any traffic can be considered benevolent and removed using the tabu-list feature of agent. The agents use pheromone deposition as the means of communication, the higher pheromone value relates to the higher probability of route selection. This feature plays an important role in deceiving the intruder by creating virtual values along the 'bait' network. Hence, an intruder who is watching the traffic will assume everything is normal and end up attacking or probing the ‘bait architecture’. Since C2SP is used as an optimization algorithm, the process of tracking the intruder while balancing the virtual and real resources and traffic prioritization is possible.

5. 2 Battlefield Monitoring

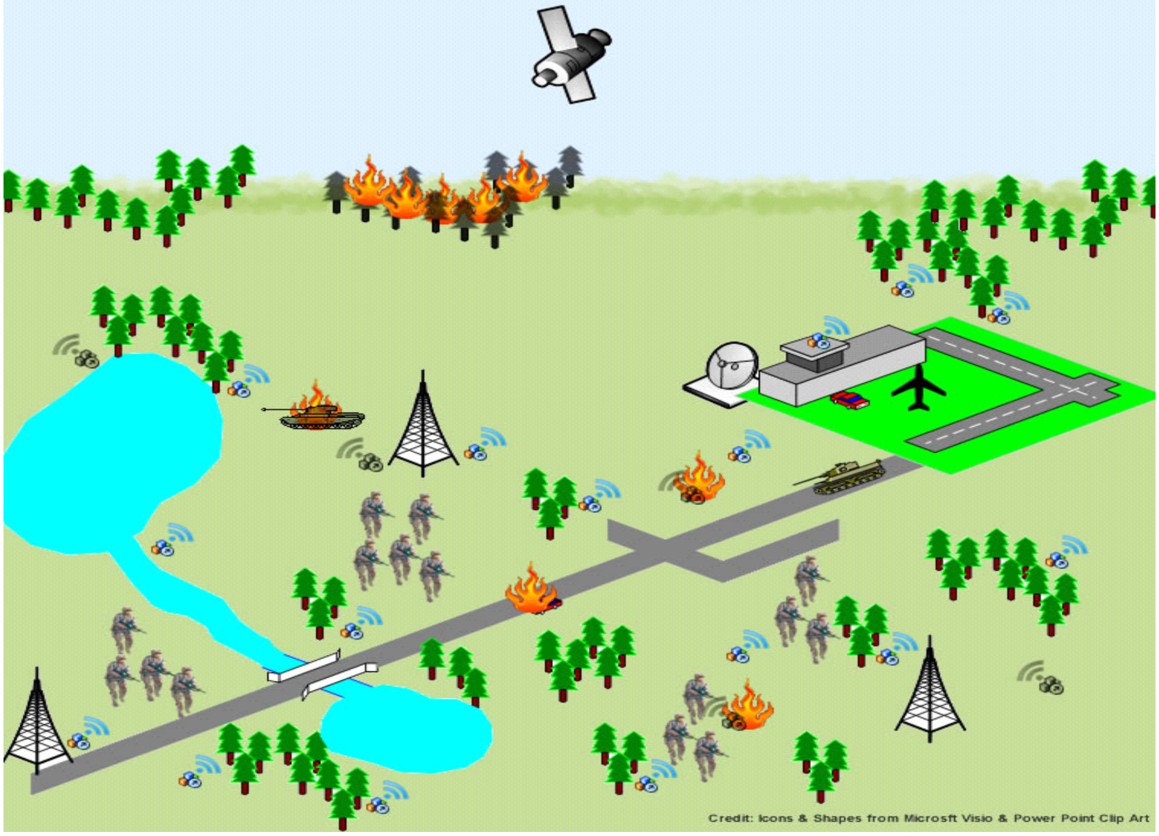

Credit: Icons & Shapes from Microsft Visio & Power Point Clip Art

Figure 5.2. Sensor based Battlefield Intrusion Detection System

Battlefield monitoring is an application that generates sensitive data. Figure 5.2 illustrates sensor network deployed in securing battlefield monitoring. There are two ways a battlefield can be monitored. First, deploying sensors in a strategic manner where part of the sensors can be used as ‘bait’ for intruders. Unfortunately, this requires good knowledge of the environment. Secondly, deploying sensors at random, but initializing agents that mimics ‘bait’ trail for intruders. In the figure below, the sensors deployed in shaded area are ‘bait’ sensors, where the message traffic is induced by the agents. Thus improving the functionality of the sensors, while balancing the resources with no prior localization knowledge.

The performance of the network is influenced by quality of data collected and processed by sensor but also the amount of time required to be transmitted to base (destination). Hence, any false positive decision may jeopardize the lives of soldiers, innocent bystanders or infrastructure. Battlefield monitoring system is initialized secretly by deploying sensors in a random manner using unmanned aerial vehicles (UAV). The primary task of these heterogeneous sensors is to capture, track and relay messages to the base regarding any movements of human or non-human objects. Sensors are deployed with overlapping sensing coverage to collect correlated data thus ensuring reliable information under individual node failure.

5.2.1 Experimental Network

A heterogeneous nodes of 50 wireless, 10 mobile and 5 wired nodes are deployed on a two-dimensional (2D) grid. Among the 50 wireless nodes, 25 of them are ‘bait’ nodes and the other 25 is called ‘normal’ nodes. Some of the assumptions on the network are as follows,

1. The wireless nodes have less power and computation cost.
2. Nodes have unique identity and are aware of ‘bait’ node existence.
3. ‘Normal’ nodes can be non-cooperative in nature.
4. No genuine traffic exist between ‘bait’ and ‘normal’ nodes.

The performance metrics such as hops, distance, BER, route, energy, latency and PDR are all recorded in the tabu-list and is communicated to the base station.

5.2.2 Simulated Attack Scenario

The training data consist of the different DoS attack such as Jamming, Sybil and Wormhole. The initial traffic is set by the base station, beyond which an unsupervised control is given to the nodes to identify any attacks.

1. ‘Bait’ nodes are cooperative in nature.
2. ‘Bait’ nodes are strictly relay nodes and the traffic is initiated by a base station.
3. ‘Bait’ nodes has same resource constraints as ‘normal’ nodes.
4. Upon detecting a traffic from illegitimate node, the ‘bait’ nodes alerts its neighboring nodes to participate in routing.
5. ‘Insider’ attacks refers to ‘normal’ nodes under malicious attack and ‘Outsider’ attacks refers to illegitimate nodes attacking either the ‘bait’ or ‘normal’ nodes.

The number of ‘normal’ and ‘bait’ nodes are kept the same to ensure fairness in detecting threats. The IDS and Bayesian network robustness is tested in environment where three new attacks such as sinkhole, black hole and misdirection.

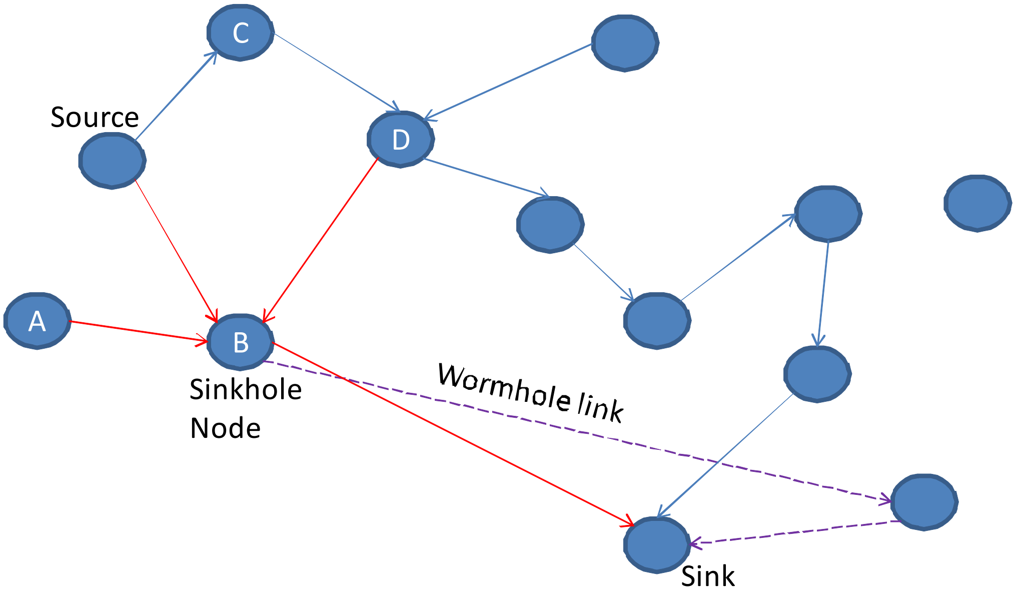


Figure 5.3. Sinkhole attack in Sensor based Network

As shown in Figure 5.3 in a Sinkhole attack, the malicious node advertises as the route with the high quality, and can spoof its neighboring nodes. Also, a sinkhole node can act like a wormhole node, by replaying message at the other end and falsely claim that it has direct connection to the base station.

In misdirection attack, the 'malicious' node corrupts the data packets that is forwarded during data transmission. Due to the route tampering, the malicious node easily re-routes data flow, thus affecting system performance and also security of data itself is jeopardized. In a Black hole attack, the malicious node advertises high energy ability to its neighbors and participates in relaying information.

In an 'active' DoS attack the malicious node actively participates in attacking the neighboring nodes to degrade the network performance, whereas in 'passive' attack, the illegitimate node attacks the route without participating often, thus reducing the probability of being detected by intelligent algorithm.

5.2.3 Simulated Results

The attack identified by the 'bait' architecture below is sinkhole where the attacker advertises with high QoS and best route to actively participate as relay node. The attack data set for Bayesian network is trained as shown in Figure 5.4. Under a sybil attack, the node (1,2) pretends dual personality as (2,1) and (3,4). In the first route, the SI algorithm is tricked in believing that (1,2) is a reliable node since there is a communication delay in detecting the DoS attack. Whereas in the next subplot the algorithm responds immediately to the attack and excludes the compromised node from its route, thus maintaining the efficiency of the network. The performance parameters have a direct impact in identifying if the node is under DoS attack. By using the negative packet delivery weight, the malicious node can be removed from the route.

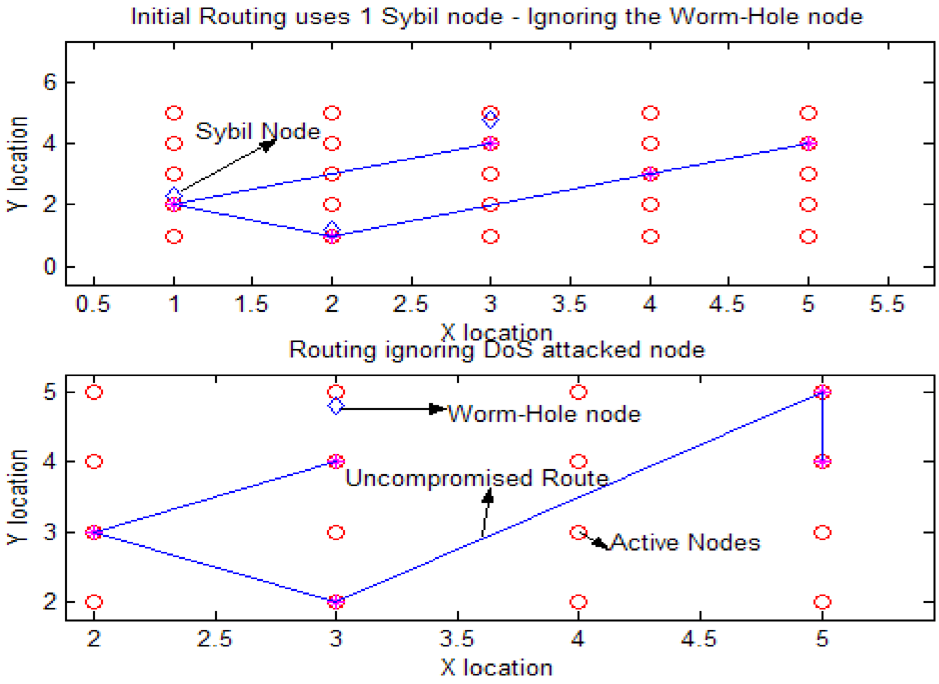


Figure 5.4. Training ‘Sybil’ and ‘Wormhole’ data set for Bayesian Network

The computation cost is an important feature to consider while evaluating the ‘bait’ architecture.

Figure 5.5 shows the detection rate of a sink hole attack is above 80%, which could be due to the fact that the model was trained with wormhole attack.

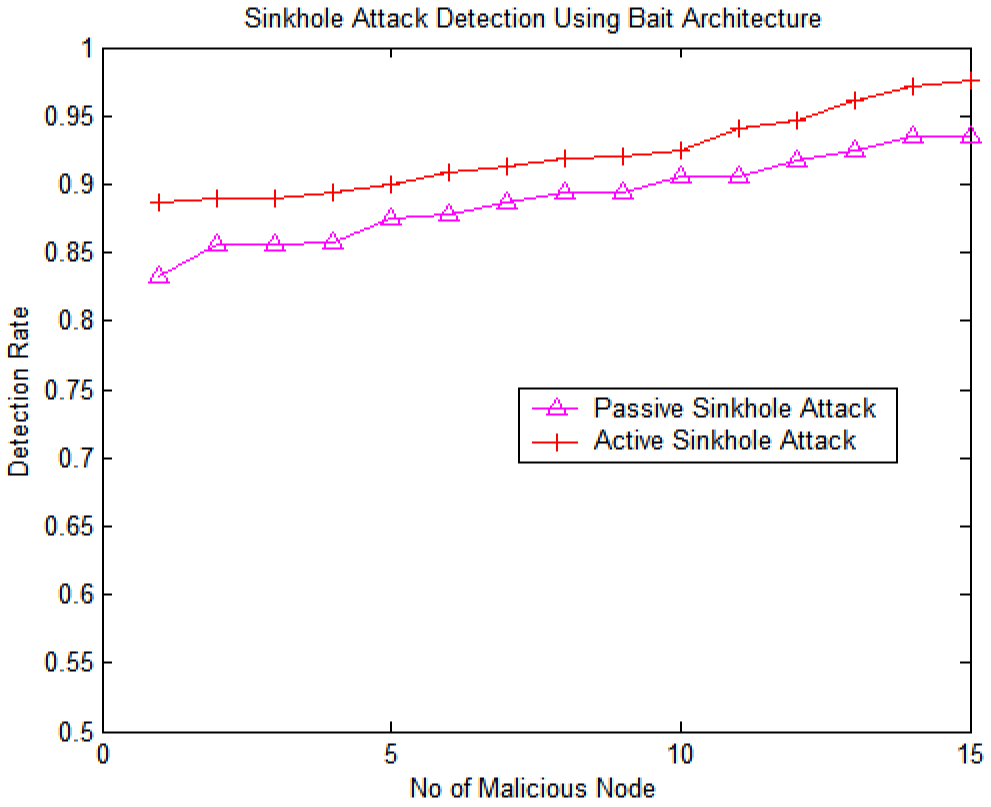


Figure 5.5. Detection of Sinkhole attack using 'Bait' Architecture

In the black hole attack, the illegitimate node advertises to have high energy and attracts traffic and can has been easily detected using the 'bait' architecture as shown in Figure 5.6. The detection rate of the passive black hole attack is also lower when compared to the active black hole attack.

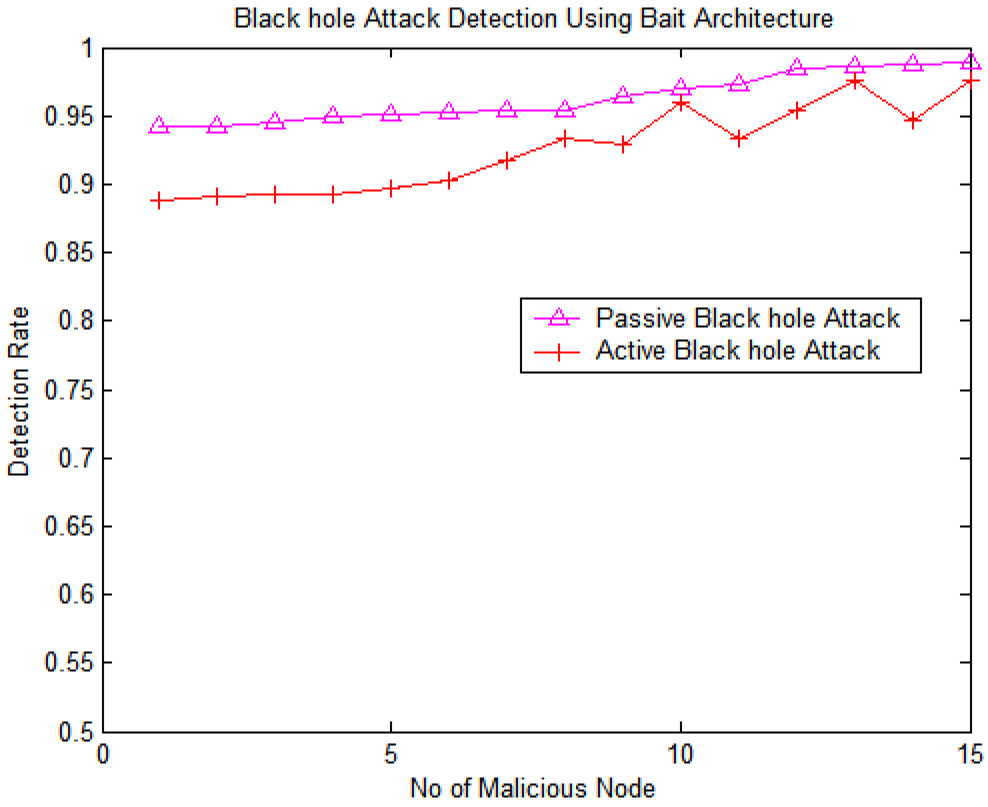


Figure 5.6. Detection of Black hole attack Using Bait Architecture

Finally, the misdirection attack that commonly happens in any distance or geographical based routing protocols such as Ad-hoc On demand Distance Vector (AODV), DSR etc. In this attack, a malicious node adds on fake route when updating the table, which leads the neighboring nodes to exhaust its resources.

Figure 5.7 shows the detection rate of the misdirection attack, and its evident that apart from a combined knowledge of the bait architecture and the robustness of the C2SP aids in identifying a discrepancy in route. As the C2SP's transition probability depends not only on a route but also on other performance factors. Thus, designing a secure protocol lies in understanding the performance metrics and application constraints.

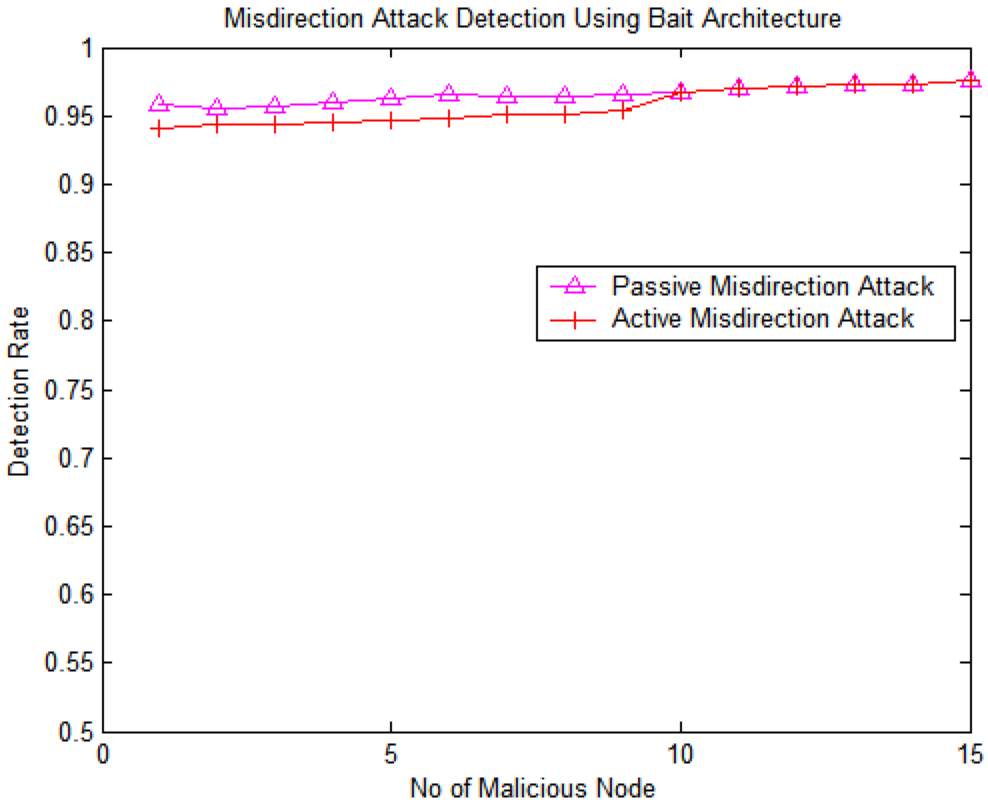


Figure 5.7. Misdirection Attack Using Bait Architecture

Figure 5.8 illustrates the performance of the two approaches, ‘bayesian’ based C2SP represented in ‘triangles’ and ‘bait’ based IDS, represented with ‘+’. The ROC curve gives the sensitivity of the application with the detection rate of the application under intruder attack. In the simulation, a jammer and wormhole attack was combined to analyze the performance of the different approaches. The Bayesian based model was trained with data set consisting of individual DoS attack such as Sybil, Wormhole and Jammer whereas the IDS was only exposed to wormhole DoS attack scenario. The models had different threshold settings throughout the simulations to enhance their learning feature. The approaches were able to detect about 90% and above for unknown DoS attack scenarios.

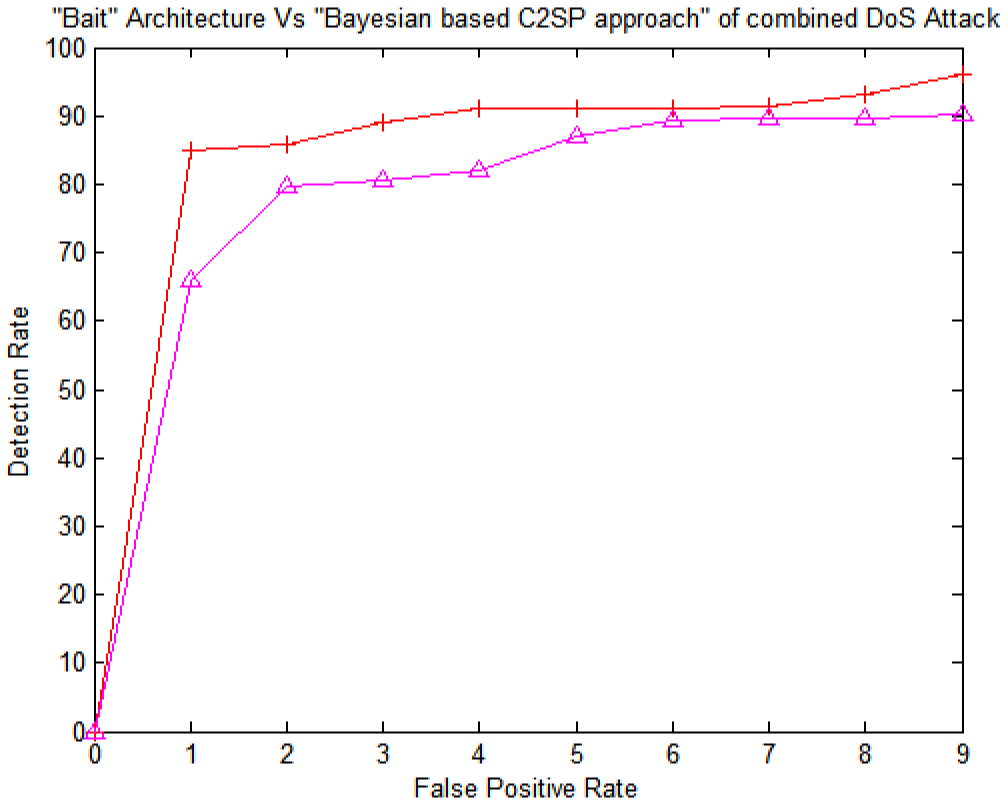


Figure 5.8. Performance Comparison Using ROC curve for Bayesian and Bait based Approach for a combined DoS attack

The successful identification of a malicious node in a combined DoS attack using ‘bait’ architecture is given in Figure 5.9. It is important to note that if the increased number of node is attacked the identification of the malicious node is down to 70% whereas, for a minimal number of attack, the identification of illegitimate node is close to 100%. A intruder system works best if a balance between a false positive and false-negative rate is found. In addition, if the sink node is at the farthest end of the network, chances of a illegitimate node is higher as the number of hops and multipath is increased and so is the vulnerability of the route.

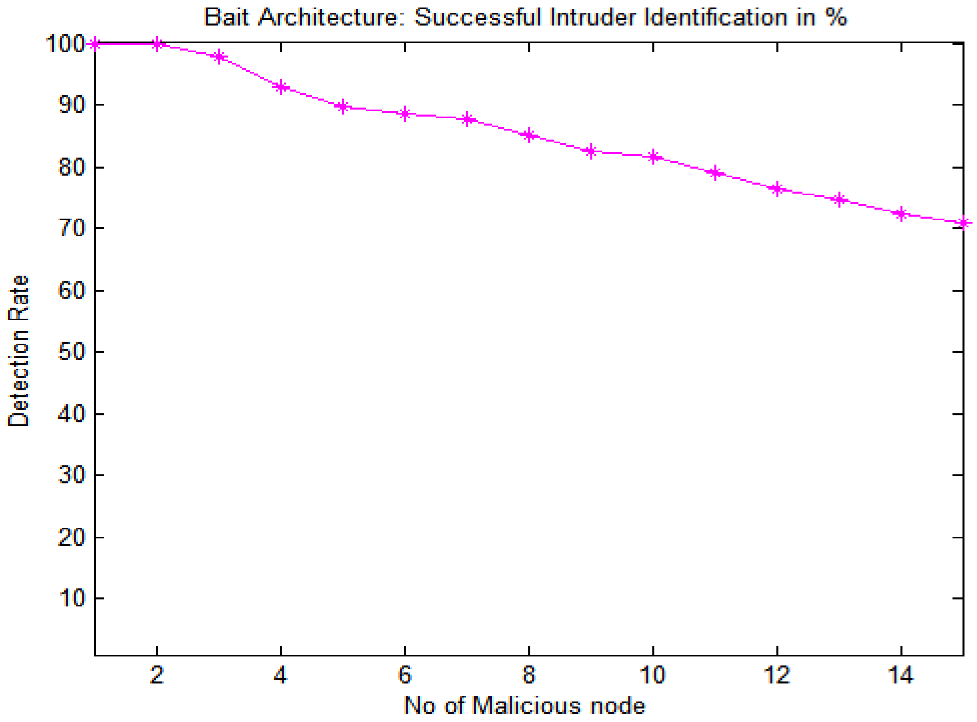


Figure 5.9. Successful Identification of Combined DoS attack Using 'Bait' Architecture

The performance of bayesian based C2SP approach and 'bait' based IDS architecture depend primarily on the application's resource availability and sensitivity. In order to achieve maximum security in critical applications such as battlefield deployment, other application where nations natural resources such as Smart Grid, Border security, Smart-care etc., require protection a 'bait' architecture is best suited. For applications such as Habitat Monitoring, etc a Bayesian model is a best fit. Also, the increased sensitivity of the application means there are some inconvenience caused to the user (customer) that needs to be tolerated for the sake of security.

5. 3 Research Conclusion

In this chapter, the importance of an IDS for sensor network is analyzed. The addition of ‘bait’ nodes with a feature to mimic traffic gives insight of adversary’s mission to attack the network.

The ‘bait’ architecture was able to predict any new DoS attack such as Sink hole, Black hole and Misdirection. The ‘bait’ architecture’s detection rate is directly proportional to the learning data set provided and the performance metrics. Battlefield monitoring application was assumed to have abundant resources and hence high-interaction ‘bait’ architecture was assumed. For time sensitive or high priority applications such as Health-monitoring, Emergency Responder etc., deploying ‘bait’ nodes are not feasible. In such scenarios, ‘super’ nodes with additional computation power can be deployed i.e., Smart home devices can actively participate in predicting an abnormal behavior.

CHAPTER SIX

Conclusion and Future Work

"Research is a cup that never runs over"

The chapter gives a brief description on the contributions made in this dissertation. The research direction can be further explored and possible extensions can be made for future research.

6. 1 Research Conclusion and Contributions

Sensors have become predominant in our day-to-day lives, where one can start a day with sensor equipped shoes to securing the borders of a nation using unsupervised nodes. Therefore, it is imperative that security must be considered during the design phase of any technology. Security schemes should be tailored to each application based on its resource availability and performance. My contribution to this research is as follows,

Background on the research in the field of sensor security in both academia and industry are discussed. An overview of all the research contributions in securing the different aspects of the sensor network are analyzed. In addition, the need for achieving security by applying simple design techniques considering performance metrics and environmental settings. There are many research work in sensor security, but detection, prediction and countermeasure for a combined DoS attack is not been explored using a cognitive approach and evaluated under different simulated scenarios. Henceforth, to date this research work is considered state-of-the-art in the field of swarm intelligence and heterogeneous sensor network

The major contribution of this dissertation is a three-fold framework that cognitively adapts its performance based on the situation and application requirements. The different types of denial-of-service attacks that can jeopardize an application is carefully considered and countermeasures are implemented. The fundamentals of swarm intelligence and features of the ant colony optimization algorithm are combined to form a security protocol. In addition, the security protocol is tailored for a wide variety of applications by weighing the performance parameters using mathematical concepts called partially ordered sets. Applications such as Emergency Responder and Health-care monitoring were simulated with scenarios similar to threats faced in the real world. The robustness and reliability of the C2SP is justified with the countermeasure solutions obtained where optimal resources such as energy, distance, hops are achieved while improving the quality of service and application performance.

In the second phase of the cognitive framework the learning feature of the agents is further enhanced using inference made by Bayesian models. Among all the other denial-of-service attacks, a jamming attack on the physical layer is considered most vulnerable and hence, detecting the same is crucial for the application. The jammer types are discussed and appropriate metrics are determined to detect abnormal behavior in sensor nodes. A good training data set for Bayesian models help detect a jammer with more accuracy, and hence application such as vehicular ad-hoc network is best suited. In addition, due to the dense deployment of nodes, and multiple monitors further improve the accuracy of jammer detection. Also an approximate location of the jammer can be obtained using the affected nodes is the area.

Finally, the third phase of the security framework is when the application requires utmost security against threats and has the resources to learn the attacker's interest about the application and data. The 'bait' architecture mimics normal traffic to gain adversary, and dedicated nodes are deployed for this purpose. The extended architecture successfully identifies new denial-of-service attacks but with a high cost. Hence, battlefield application where national security could afford the resources is considered. The pattern learnt from an adversary depends on the type of 'bait' architecture used. Thus, the three fold cognitive framework balances between defending, and detecting a threat to the network based on the application constraints and performance requirements.

Chapter 2 analyses the different active research performed in the field of security. In Chapter 3, a detailed background on the security such as data, network and application was discussed. And the different approaches taken by researchers to defend the network was explained. Chapter 4 gives a overview of the evolutionary algorithm, and its role in C2SP. In addition, the weights on performance metrics is applied to obtain mission-critical optimal solutions using POSets. The learning feature of the C2SP is further explored using Bayesian network to detect a threat and locate its origin in Chapter 5. The final phase of the proposed cognitive framework, where a 'bait' architecture to predict future attacks is discussed in Chapter 6. In each of the chapters, an application that exist in real-world is analyzed and simulated to justify the proposed framework's reliability, robustness and versatility. In addition, the cognitive framework is not only adaptive to the different security threats but also to any application formulated. The best feature of the proposed framework, is the ability to learn from its environment and also to refine its solutions by adapting to the application requirements and constraints.

The proposed novel framework controls heterogeneous sensor network requirements, and balance the resources optimally and efficiently while communicating securely using a multi-objection function. In addition, the framework can measure the affect of single or combined denial of service attacks and also predict new attacks under both cooperative and non-cooperative sensor nodes. The cognitive intuition of the framework is evaluated under different simulated real time scenarios such as Health-care monitoring, Emergency Responder, VANET, Biometric security access system, and Battlefield monitoring.

6. 2 Future Work

The contribution for the security in sensor network are as follows

1. Countermeasure for denial-of-service attack,

2. Detecting a denial-of-service attack,

3. Predicting ‘new’ denial-of-service attack and

4. Cross-Layered Cognitive Security Protocol.

Hence, the future research direction in these three sections are as follows,

6.2.1 Countermeasure Against DoS attack

Chapter 3 discusses countermeasure against DoS attack in both sensor based health-care monitoring and emergency responder application. Although, the application here is assumed to have location information, in reality people originating from rural and suburban have different types of connectivity to the web. Hence, not all devices can be connected to the network and an accurate location information is close to impossible, and so is the time synchronization of information among nodes. The source and sink nodes where always considered secure, and a cooperative nature within the network is observed, which needs to be extended to insider attacks.

6.2.2 Detecting of DoS attack

The detection of DoS attack was analyzed assuming a complete knowledge of the intruder and application. In many cases, an unpredictable node behavior is caused by environment and most sensor nodes are applied in remote areas where monitoring their conditions is not feasible. Hence, a minimally trained bayesian network with the ability to learn from its past using feature extraction can be further explored. Also, the location of a jammer is an interesting idea, but a centroid location based on neighboring DoS attacked nodes will result in very high false positives. As nodes involved in DoS claims can be from illegitimate and genuine nodes, and hence an extensive method of locating jammer not only based on claims but also mathematical models would increase location detection accuracy.

6.2.3 Predicting DoS attacks

The process of adding ‘bait’ architecture for resource available networks restricts the safety of resource constrained networks. Hence, the nodes can rather have different functionality and switch modes in either being a relay, source, sink or ‘bait’ nodes based on the situation assessment. Also, the current framework helps in predicting new DoS attacks, which can be further extended to predicting data, network and application security attacks.

6.2.4 Cross-Layered Cognitive Security Protocol

The C2SP approach consist of concepts from ant colony optimization (ACO) and partially ordered sets (POSets), together with a layered feature of network model. The generic structure of C2SP can be modeled independent of any application. In essence, by adding more features to the C2SP, the characteristics such as de-centralization, unsupervised, reachability, reliability, versatility and robustness should be maintained. Security threats are constantly evolving so the exploratory behavior of agents must adapt and evolve in accordance. A balance of exploration and exploitation is the key for cognitive intelligence.

Bibliography

[1] C. Wang, C. Lee, H. Chu, "Optimal Deployment for Wireless Sensor Networks Using Lifetime Expectation Estimation," Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007), vol. 1, pp.15-18, 2007

[2] L. Lazos, R. Poovendran, and J. A. Ritcey, “On the Deployment of Heterogeneous Sensor Networks for Detection of Mobile Targets”, Fifth International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2007.

[3] R. Muraleedharan and L. Osadciw, “ Decision Making in a Building access system Using Swarm intelligence and Posets“, 38th Annual Conference on Information Sciences and Systems, 2004.

[4] S. Hussain, A. Matin, “ Base Station Assisted Hierarchical Cluster-Based Routing”, ICWMC, 2006.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy- Efficient Communicat ion Protocol for Wireless Microsensor Networks”, Proceedings of the Hawaii International Conference on System Sciences, 2000.

[6] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, and D.Rubenstein, “Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with zebranet,” in Proceedings of ASPLOS-X. ACM, 2002.

[7] C. Guestrin, A. Krause, and A. P. Singh, “Near-optimal sensor placements in gaussian processes,” in ICML, 2005.

[8] J. Tay, V. Chandrasekhar, W. Seah, “ Selective Iterative Multilateration for Hop Count-Based Localization in Wireless Sensor Networks”, 7th International Conference on Mobile Data Management, 2006.

[9] Vaidyanathan Ramadurai and M. L. Sichitiu, "Localization in wireless sensor networks: A probabilistic approach", in Proc. of the 2003 International Conference on Wireless Networks (ICWN 2003), Las Vegas, NV, June 2003, pp. 275-281

[10] AWAIRS: Adaptive Wireless Arrays for Interactive Reconnaissance, Surveillance, and Target Acquisition in Small Unit Operations. http://www.janet.ucla.edu/awairs, 2000.

[11] Asada, G., Dong, M., Lin, T., Newberg, F., Pottie, G., Marcy, H., and Kaiser, W. Wireless integrated network sensors: Low-power systems on a chip. In Proceedings of the 24th IEEE European Solid-State Circuits Conference . 1998.

[12] Smart Dust: Autonomous Sensing and Communication in a Cubic Millimeter. http://robotics.eecs.berkeley.edu/~pister/SmartDust, 2000.

[13] J. Kahn, R. Katz, and K. Pister. Mobile Networking for Smart Dust. In Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99), August 1999.

[14] A. Mainwaring, J. Polastre, R. Szewczyk, and D. Culler, “Wireless Sensor Networks for Habitat Monitoring”, IRB-TR-02-006, June, 2002.

[15] CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care, David Malan, Thaddeus Fulford-Jones, Matt Welsh, Steve Moulton, MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES 2004), June, 2004.

[16] R. Muraleedharan and L. A. Osadciw,”Security: Cross Layer Protocol in WSN”, INFOCOM 2006, Spain.

[17] A.D. Wood, J.A. Stankovic and S.H. Son “JAM: A Jammed-Area Mapping Service for Sensor Networks“, In Real-Time Systems Symposium (RTSS), Cancun, Mexico, 2003.

[18] R. Muraleedharan, Y. Yan, L.A. Osadciw, ” Detecting Sybil Attacks in Image Sensor Network Using Cognitive Intelligence", SANET, Mobicom Workshop, Montreal, Canada, September 2007.

[19] J. Newsome, E. Shi, D. Song, A. Perrig, “The Sybil Attack in Sensor Networks: Analysis and Defenses“, Third International Symposium on Information Processing in Sensor Networks (IPSN), 2004.

[20] H. Alzaid, E. Foo, J. G. Nieto , “Secure data aggregation in wireless sensor network: a survey”, Proceedings of the sixth Australasian conference on Information security - Volume 81, 2008.

[21] L. Eschenauer , V. D. Gligor, “A key-management scheme for distributed sensor networks”, Proceedings of the 9th ACM conference on Computer and communications security, Nov. 2002.

[22] W. Du , J. Deng , Y. S. Han , P. K. Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, Proceedings of the 10th ACM conference on Computer and communications security, Oct 2003.

[23] K. Okeya and T. Iwata, "Side channel attacks on message authentication codes," 2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks, July 2005

[24] S. Zhu, S. Setia, and S. Jajodia, "Leap: efficient security mechanisms for large-scale distributed sensor networks," in CCS '03: Proceedings of the 10th ACM conference on Computer and communications security. New York, NY, USA: ACM Press, 2003, pp. 62–72.

[25] D. McIntire, K. Ho, A. Singh, W. Wu, and W.J.Kaiser, "The low power energy aware processing (LEAP) embedded networked sensor system", Proc. of the 5th international conference on Information processing in sensor networks, 2008.

[26] A. Perrig, R. Canetti, D. Song, and D. Tygar., "The TESLA Broadcast Authentication Protocol.", In RSA Cryptobytes, Summer 2002.

[27] D. Liu, and P. Ning., " Multi-Level μTESLA: Broadcast Authentication for Distributed Sensor Networks", ACM Transactions in Embedded Computing Systems, 2004.

[28] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D.Tygar., " Spins: Security protocols for sensor networks". Wireless Networks, 8:521 – 534, 2002.

[29] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Wireless Mobile Networks," in Ninth Internation Conference on Network Protocols (ICNP'01), 2001, pp. 251– 260.

[30] Q. Zhang, X. Zhou, F. Yang, " Distributed node authentication in wireless sensor network", Proc of the 5th international conference on wireless communication, networking and mobile computing, 2009.

[31] Y. Ouyang, Z. Le, Y. Xu, N. Triandopoulos, " Providing Anonymity in Wireless Sensor Networks", In Proceedings of IEEE International Conference on Pervasive Services (ICPS), Istanbul, Turkey, July 2007.

[32] C. Karlof, N. Sastry, and D. Wagner, " TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", ACM SenSys 2004.

[33] S. Ganeriwal and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," presented at the 2nd ACM workshop on Security of ad hoc and sensor networks Washington DC, USA 2004.

[34] A.D. Wood and J.A. Stankovic, “Denial of Service in Sensor Networks“, IEEE Computer, Vol 35, Issue: 10, Oct 2002.

[35] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In MobiHoc '05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pages 46-57, New York, NY, USA, 2005. ACM Press.

[36] Anthony D. Wood, John A. Stankovic, Gang Zhou, “DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks,” in The 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), San Diego, CA, June 2007.

[37] Y.C. Tay, K.Jamieson, H. Balakrishnan, “Collision-minimizing CSMA and Its Applications to Wireless Sensor Networks”, IEEE Journal on Selected Areas in Communications, Volume: 22, Issue: 6, Pages: 1048 – 1057, Aug. 2004.

[38] M. Cagalj, S. Capkun, J. Hubaux, “Worm-hole based Antijamming Techniques in Sensor Networks”, IEEE Transactions on Mobile Computing, Vol 6 Iss. 1, pg 100-114, 2007.

[39] F. Wang, O. Younis, M. Krunz, “GMAC: A game-theoretic MAC Protocol for Mobile Ad-hoc Networks”, Modeling and Optimization in Mobile, Ad-hoc and Wireless Networks, 4th Intl Syposium, Apr 2006.

[40] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” Communications of the ACM, vol. 24, no. 2, pp. 84–90, 1981.

[41] X. Wu, “Ao2p: Ad hoc on-demand position-based private routing protocol,” IEEE Transactions on Mobile Computing, vol. 4, no. 4, pp. 335–348, 2005, fellow-Bharat Bhargava.

[42] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, and K. Jones, “On providing anonymity in wireless sensor networks.” in 10th International Conference on Parallel and Distributed Systems (ICPADS 2004), 7-9 July 2004, Newport Beach, CA, USA, 2004, pp. 411–418.

[43] C. Karlof and D.Wagner, “Secure Routing in Sensor Networks: Attacks and Countermeasures“, First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[44] Y. Zhang , and W. Lee, " Intrusion detection in wireless ad-hoc networks", Pages: 275 - 283 Year of Publication: 2000 ISBN:1-58113-197-6, ACM, 2000.

[45] R.A. Wasniowski, “ Multi-sensor agent-based intrusion detection system”, In Proc of the 2nd annual conference on Information Security Curriculum development, 2005.

[46] A. Agah, K. Basu, and S.K. Das, “ Preventing DoS attack in Sensor Network: a game theoretic approach”, ICC 2005.

[47] Y. an Huang and W. Lee, A cooperative intrusion detection system for ad hoc networks, in Proc of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, 2003, pp. 135–147.

[48] R. Roman, J. Zhou, J. Lopez, “ Applying Intrusion Detection Systems to Wireless Sensor Networks”, CCNC, 2006.

[49] E. Bonabeau, M. Dorigo, and G. Théraulaz, “ Swarm intelligence: from natural to artificial systems”, Oxford University Press, 1999.

[50] Marco Doringo, “The Ant System: Optimization by a Colony of Cooperating Agents“, IEEE Transactions on Systems, Man and Cybernetics-Part B, Vol-26, No. 1, Sept1996,pp 1-13.

[51] B. R. Secrest, “ Traveling Salesman Problem for Surveillance Mission using Particle Swarm Optimization ”, Thesis , School of Engineering and Management of the Air Force Institue of Technology, Air University , 2001.

[52] R. Muraleedharan, L.A.Osadciw, “Cognitive Routing Protocol for Sensor Based Intelligent Transportation System”, Book titled: Wireless Technologies for Intelligent Transportation Systems, Editors. M. Zhou, Y. Zhang and L.T.Yang, Nova Science Publisher, USA, 2008.

[53] R. Muraleedharan, X. Ye and L.A. Osadciw, “Prediction of Sybil Attack on WSN Using Bayesian Networks and Swarm Intelligence”, Wireless Sensing and Processing 2008, Orlando, FL, Mar. 2008

[54] V. Kawadia and P. R. Kumar, “A Cautionary Perspective on Cross Layer Design”, Submitted to IEEE Wireless Communication Magazine. July 9, 2003.

[55] Zheng-Yu Wu, Han-Tao Song, “Ant-based Energy-aware Disjoint Multipath Routing Algorithm for MANETs”, The Computer Journal Advance Access, Oxford University, Feb 2008.

[56] C. Barrett, A. Marathe, M. V. Marathe, M. Drozda, “Characterizing the interaction between routing and MAC protocols in ad-hoc networks”, International Symposium on Mobile Ad-Hoc Networking and Computing, Proceedings of the 3rd ACM international symposium on mobile ad hoc networking and computing, Lausanne, Switzerland, 2002, Pages 92.103.

[57] Woodward, P. M., Probability and Information Theory, with Applications to Radar, Pergamon Press, Inc., NY 1953.

[58] Muraleedharan R., Osadciw L.., “Secure Health Monitoring Network Against Denial-Of-Service Attacks Using Cognitive Intelligence” Communication Networks and Service Research Conference, CNSR, Halifax, Canada, 2008.

[59] Muraleedharan R., Gao W, Osadciw L.A., “Swarm Intelligence Managed UWB Waveform and Cognitive Sensor Network Protocol”, IEEE Swarm Intelligence Symposium, St. Louis, Missouri, March 2009.

[60] August N.J.,”Medium Access Control in Impluse-Based Ultra Wideband Ad-Hoc and Sensor Networks”, PhD Thesis, Dept of Elec. Engg, May 2005, Virginia Tech.

[61] Muraleedharan R., Osadciw L.., “An Intrusion Detection Framework for Sensor Networks Using Ant Colony”, ASILOMAR, Pacific Grove, CA, Nov 2009.

[62] Muraleedharan R., Osadciw L.A., “ Balancing The Performance of a Sensor Network Using an Ant System “, 37th Annual Conference on Information Sciences and Systems, John Hopkins Unversity, 2003.

[63] Gao W., Osadciw L.A., “A MUI Deduction Pulse Shape Design Scheme for UWB Communications", Proc. 7th IEEE Upstate New York Workshop on Communications, Sensors and Networking, Syracuse, NY, Nov. 2007.

[64] Technical Information of Bluetooth: Official website www.bluetooth.com.

[65] Technical Information of Zigbee: official website www.zigbee.org

[66] Poisel Richard, “Modern communications jamming principles and techniques“.

[67] F.C.M. Lau and C.K. Tse, " Study of Anti-Jamming Capabilities of Chaotic Digital Communication Systems," Proceedings, 2002 International Symposium on Nonlinear Theory and Its Applications, (NOLTA'2002), October 2002, Xian, China, pp.65-68.

[68] K.D.Wong, “Physical Layer considerations for Wireless Sensor Networks“, IEEE Int’l Conference Net, Sensing and Control, Mar 2004, pp 1201-1206.

[69] Steven M. Kay, “Fundamentals of Statistical Signal Processing: Detection Thory“, Vol II, Prentice-Hall Inc, 1998

[70] Muraleedharan R., Osadciw L.A., “ Jamming Attack Detection and Countermeasures In WSN using Swarm Intelligence”,Defense and Security Symposium, March 2006.

[71] Muraleedharan R., Yan Y, Osadciw L.A., “Constructing on Efficient Wireless Face Recognition System by Swarm Intelligence”, SCI journal, 2007.

[72] Ting Shan, Brian C. Lovell and Shaokang chen, “ Person Location Service on the Planetory Sensor Network “, APRS Workshop on Digital Image Computing, 21 Feb 2005 (1), Brisbane, Pg 151-156.

[73] Yan. Y, Osadciw L.A., “Contourlet Based Image Recovery and De-noising Through Wireless Fading Channels“, 39th Annual Conference on Information Sciences and Systems, John Hopkins Unversity, 2005.

RAJANI MURALEEDHARAN

4823 Bear Road, Apt #10B, Liverpool, NY 13088.
Phone: (315) 289-7933
Email: rmuralee@gmail.com
Website: www.cognitiveintelligence.com

PROFILE

- PhD in Electrical & Computer Science Engineering at Syracuse University.
- Extensive research in Bio-Inspired algorithm using interdisciplinary approach on performance metrics and multi-objective optimization problems.
- Extensive research in Routing and Security Strategies in Wireless Sensor Networks.
- Rich teaching experience in graduate and undergraduate level courses on diverse subjects.
- Published 1 Book Chapter, 3 Journal Articles and 24 peer reviewed articles (2 Best Paper Awards).
- Awarded 2009 Outstanding Teaching Assistant at University Level (Top 4%).
- Awarded 2009 Certificate in University Teaching (CUT) by Future Professoriate Program.

EDUCATION

- Doctorate of Philosophy..August 2011
  Electrical Engineering, Syracuse University
  Dissertation topic: Cognitive Security Framework for Heterogeneous Sensor Network Using Swarm Intelligence

- Illinois Wireless Summer School...June 2009
  University of Illinois at Urbana-Champaign

- Master of Science..May 2005
  Computer Engineering, Syracuse University
  Project Title: Cognitive Routing Protocol for Sensor Based Intelligent Transportation System

- Diploma in Ecommerce...May 2001
  Anna University

- Bachelor of Engineering..May 2000
  Computer Science & Engineering, University Of Madras
  Project Title: Airline Landing Charges

RESEARCH EXPERIENCE

- Research Intern...Jul – Oct 2010
  Mitsubishi Electric Research Laboratories, Cambridge MA
- Research Assistant/Associate..August 2002- May 2010
  Dreamsnet Research Lab, Syracuse University, Syracuse NY

TEACHING EXPERIENCE

- Teaching Associate...August 2005 – May 2010
  L.C. Smith College of Engineering & Computer Science, Syracuse University
- Instructor (Future Professoriate Program)..Fall 2007
  L.C. Smith College of Engineering & Computer Science, Syracuse University

PUBLICATIONS

Book Chapter:

- Cognitive Routing Protocol for Sensor Based Intelligent Transportation System
  Rajani Muraleedharan and Lisa Ann Osadciw, book titled, "Wireless Technologies for Intelligent Transportation Systems", Ming-Tuo Zhou, Y. Zhang and Laurence T. Yang (Editor), Nova Science Publishers, USA, 2008

Journals:

- Resource Optimization in Distributed Biometric Recognition Using Wireless Sensor Network
  Rajani Muraleedharan, Dr. Lisa Ann Osadciw and Yanjun Yan, Multidimensional Systems and Signal Processing Journal, 2009.
- SmartCare: Health Monitoring Using Wireless Sensor Networks
  Rajani Muraleedharan and Dr. Lisa Ann Osadciw, Special Issue: Pervasive Health Care Services and Technologies, International Journal of Telemedicine and Applications, 2008.
- Constructing on Efficient Wireless Face Recognition System by Swarm Intelligence
  Rajani Muraleedharan, Yanjun Yan and Dr. Lisa Ann Osadciw, SCI journal, 2007.

Peer Reviewed Conference Papers:

- Bio-Inspired Secure Data Mules for Medical Sensor Network
  Rajani Muraleedharan, and Lisa Ann Osadciw, SPIE Defense and Security, Orlando, FL, Mar 2010.
- An Intrusion Detection Framework for Sensor Networks Using Ant Colony
  Rajani Muraleedharan, and Lisa Ann Osadciw, ASILOMAR, Pacific Grove, CA, Nov 2009.
- Secure Self-Adaptive Framework for Distributed Smart Home Sensor Network
  Rajani Muraleedharan, and Lisa Ann Osadciw, ASILOMAR, Pacific Grove, CA, Nov 2009.
- Cognitive Security Protocol for Sensor Based VANET Using Swarm Intelligence
  Rajani Muraleedharan, and Lisa Ann Osadciw, ASILOMAR, Pacific Grove, CA, Nov 2009.
- Secure Self-Adaptive Mission Critical Framework for Distributed Smart Home Sensor Network
  Rajani Muraleedharan, and Lisa Ann Osadciw, MobiQuitious, Toronto, Canada, July 2009.
- Secure Communication in Heterogeneous Sensor Networks
  Rajani Muraleedharan, and Lisa Ann Osadciw, MobiQuitious, Work-in-Progress, Toronto, Canada, July 2009.
- Swarm Optimized UWB-PPM and Protocol design for sensor network
  Rajani Muraleedharan, Weihua Gao and Dr. Lisa Ann Osadciw, SPIE Defense and Security Symposium,Orlando, FL, April 2009.
- Swarm Intelligence Managed UWB Waveform and Cognitive Sensor Network Protoco
  Rajani Muraleedharan, Weihua Gao and Dr. Lisa Ann Osadciw, IEEE Swarm Intelligence Symposium, St. Louis, Missouri, March 2009
- Meta-heuristic Cross-Layer Protocol for UWB Emergency Responder Sensor Network
  Rajani Muraleedharan, Weihua Gao and Dr. Lisa Ann Osadciw, IEEE Swarm Intelligence Symposium, St. Louis, Missouri, September 2008
- Secure Health Monitoring Network Against Denial-Of-Service Attacks Using Cognitive Intelligence -BEST PAPER AWARD

Rajani Muraleedharan and Dr. Lisa Ann Osadciw, Communication Networks and Service Research Conference, CNSR, Halifax, Canada, 2008

- Predicting Sybil Attack in Wireless Sensor Network using Swarm-Based Reasoning Algorithm

  Rajani Muraleedharan, Xiang Ye and Dr. Lisa Ann Osadciw, SPIE Defense and Security Symposium, Orlando, FL, March 2008
- Ant System Based Flexible and Cost Effective Routing for Wireless Face Recognition

  Rajani Muraleedharan, Yanjun Yan and Dr. Lisa Ann Osadciw, CCNC, Las Vegas, NV, 2008
- Contourlet Based Image Compression for Wireless Communication in Face Recognition System

  Yanjun Yan, Rajani Muraleedharan and Dr. Lisa Ann Osadciw, ICC, Beijing, China, May 2008
- Detecting and Countermeasures Against Denial Of Service Attack in WSN Using Cross Layer Cognitive Protocol -INVITED

  Rajani Muraleedharan and Dr. Lisa Ann Osadciw, Doctoral Symposium, ACM Compute 2008, Bangalore, India. January 2008.
- Increasing QoS and Security in 4G Network using Cognitive Protocol

  Rajani Muraleedharan and Dr. Lisa Ann Osadciw, IEEE GLOBECOM, Washington D.C., November 2007.
- Cross Layer Protocols in Wireless Sensor Networks (Poster)

  Rajani Muraleedharan, Yanjun Yan and Dr. Lisa Ann Osadciw, SANET First ACM Workshop, Montreal, Quebec, September 2007.
- Cross Layer Protocols in Wireless Sensor Networks

  Rajani Muraleedharan and Dr. Lisa Ann Osadciw, IEEE Infocomm Student Workshop, April 2006.
- Jamming Attack Detection and Countermeasures In WSN using Swarm Intelligence

  Rajani Muraleedharan and Dr. Lisa Ann Osadciw, Defense and Security Symposium, April 2006.
- Cross Layer Denial of Service Attacks in Wireless Sensor Network Using Swarm Intelligence

Rajani Muraleedharan and Dr. Lisa Ann Osadciw, 40th Annual Conference on Information Sciences and Systems, March 2006.

- Robust Face Recognition System Constructed by Wireless Sensor Networks -BEST PAPER AWARD

  Rajani Muraleedharan, Yanjun Yan and Dr. Lisa Ann Osadciw, 9th World Multiconference on Systemics, Cybernetics and Informatics, July 2005. 'Best Paper Award' for applications in electrical engineering.
- Robustness of Predictive Sensor Network Routing in Fading Channels

  Rajani Muraleedharan and Dr. Lisa Ann Osadciw, Defense and Security Symposium, March 2005.
- A Predictive Sensor Network Using Ant System

  Rajani Muraleedharan and Dr. Lisa Ann Osadciw, Defense and Security Symposium, April 2004.
- Decision Making In a Building Access System Using Swarm Intelligence & POSets

  Rajani Muraleedharan and Dr. Lisa Ann Osadciw, 38th CISS conference, Princeton, NJ, March 2004
- Balancing the Performance of a Sensor Network Using an Ant System

  Rajani Muraleedharan and Dr. Lisa Ann Osadciw, 37th Annual CISS conference, Baltimore, March 2003.

AWARDS/HONORS

- Best Paper Award – Research work in Wireless Sensor Network Security – 2005 & 2008
- Awarded Women In Science & Engineering (WISE) fellow for excellence in engineering in 2008 & 2009.
- NSF Travel fund, Illinois Summer School, UIUC, Summer 09.
- Travel Grant Recipient, IEEE Swarm Intelligence Symposium 2008
- Outstanding Teaching Associate Award (OTA), Syracuse University, L.C. Smith College of Engineering, University-Wide recognition, 2009.
- Certificate in University Teaching, Teaching Associate, Future Professoriate Program, (3 of 45 EECS teaching Assistants) 2009.
- Graduate Research Associate – Fall 09, Fall 02-May 05.

- Graduate Teaching Assistant – Spring 2006
- Chosen by Who's who in Marquis.

PROFESSIONAL SERVICE/AFFILIATIONS

Program Committee:

- 25th Queen's Biennial Symposium on Communications (QPSC 2010), Canada.
- FTRG Intl Symposium on Advances in Cryptography, Security and Applications for Future Computing 2010.

Session Chair:

- Mobiquitious, Sensor Fusion Workshop 2009 – 'Event-based Mechanism'.

Review Committee:

- ACM Transaction on Embedded Computing System
- IEEE Transactions on Vehicular Technology
- IEEE Transactions on Evolutionary Computation
- IEEE Wireless Communication Magazine
- International Journal of Communication Systems
- International Journal of Molecular Sciences (MDPI)
- Wiley Security and Communication Networks
- FTRG ACSA 09
- Springer Communication Journal
- Springer Security Journal

Student Organizing coordinator:

- IEEE Sensor Network Workshop 2003, 2005 and 2007.

Member:

- Institute of Electrical and Electronics Engineering (IEEE),
- Association for Computing Machinery (ACM) and
- Society of Photo-Optical Instrumentation Engineering (SPIE), since 2004.
- Women in Science and Engineering (WISE), since 2006

SERVICES

University Service:

- Elected Graduate Representative for Tenure and Promotions Committee – Fall 2009 – Summer 10
- Elected Graduate Representative for Committee on Academic Affairs – Fall 2007 – Summer 09
- Treasurer – Group Of VLSI Enthusiast (GROVE), Syracuse University, Fall 2008- Summer 2009
- Assisted in organizing IEEE Upstate New York Workshop on Communications, Sensors and Networking, 2004, 2005 and 2007.

Leadership Activities:

- Invited Guest Speaker, ‘Technology Day for Girls’, Girl Scouts NYPENN Pathways, Syracuse, NY
- Invited Guest speaker and judge at Science, Engineering, Communication, Mathematics and Enrichment (SECME) Competition, Middle school, Syracuse, NY. 2008 & 2009.
- Mentoring Speaker, ‘Why Graduate School?’, SUNY Morrisville State College, Morrisville, NY, 2008
- Guest Speaker, ‘Life in Graduate School & Mentoring’, SUNY OSWEGO State College, Oswego, NY, 2008