Protocol Design for Counter-Measure of Various Attacks

1Shubhangi Singh, 2Riya Tyagi, 3Rajat Prajapati, 4Reetika Sahu, 5Ranjit Kumar

1Student, Information Technology Dept. Of Galgotias College of Engg and Tech., Greater Noida, Uttar Pradesh, India
1Shubhangi3may@gmail.com

2Student, Information Technology Dept. Of Galgotias College of Engg and Tech., Greater Noida, Uttar Pradesh, India
2riyatyagimps@gmail.com

3Student, Information Technology Dept. Of Galgotias College of Engg and Tech., Greater Noida, Uttar Pradesh, India
3Rajatprajapati2016@gmail.com

4Student, Information Technology Dept. Of Galgotias College of Engg and Tech., Greater Noida, Uttar Pradesh, India
4Reetikasahu6@gmail.com

5Assistant Professor, Information Technology Dept. Of Galgotias College of Engg and Tech., Greater Noida, Uttar Pradesh, India
5Ranj.kumar@galgotiacollege.edu

Abstract-- The border surveillance wireless sensor networks (WSNs) are deployed in unattended and hostile environments. This among other issues such as unreliable wireless medium used and the constrained resources (limited energy, processing ability, and storage capacity) on the tiny sensor devices pose a challenge in designing security mechanisms for the WSN. To eliminate authentication overhead, most WSN protocols assume a high level of trust among the communicating nodes. However, this creates the danger of adversaries introducing malicious nodes to the sensor network or manipulates existing ones and then subsequently use them to propagate a wide range of attacks. Detection and isolation of malicious or malfunctioning nodes in border surveillance WSN is a major security issue. It's crucial to detect and exclude these nodes in the sensor network to avoid the catastrophic decision being made as a result of falsified information injected by the adversary as well as prevent an array of attacks that can emanate from malicious nodes. Attacks emanating from malicious nodes are the most dangerous attacks. These necessitate that their detection and isolation be given top priority as malicious nodes can send erroneous or falsified reports (Byzantine problem) to the base station leading to a disastrous decision; such as, a battlefield surveillance WSN a misleading report about the enemy operations may result to extra casualties.

Index Terms: Wireless sensor network, Stop Transmit and Listen, Weighted Trust Evaluation Scheme
I. INTRODUCTION

Wireless sensor network (WSN) consists of a large number of spatially distributed autonomous sensor nodes working cooperatively to monitor the surrounding physical phenomena or environmental conditions (monitored target) and then communicate the gathered data to the main central location through wireless links. A sensor node, also known as mote is defined as a small, low-powered, wireless device, capable of gathering sensory information, perform limited data processing and transmit the gathered information to other nodes in the network via optical communication (laser), radio frequencies (RF) or infrared transmission media. A sensor node senses physical -phenomena like light, temperature, humidity, pressure, chemical concentrations, and any other phenomenon capable of causing the transducer to respond to it. Once the phenomena are sensed, the data collected (measurement) is converted into signals for further processing to reveal some characteristics on to and phenomenon from the target area (Hussain, et al., April, 2013). Another scheme that has been used in the detection and isolation of malicious nodes is Stop Transmit and Listen (STL). STL employs non-transmission times to detect malicious nodes; nodes transmitting during these times exhibit malicious behavior. STL has a drawback in that when the whole network or a major portion of it stopped their transmission at a time (during the non-transmission time) and then resume transmission, congestion and unwanted delay in the network operations arises. In this research, we propose an enhanced WTE based detection algorithm that aims to address the drawback of the WTE scheme by employing STL. The STL will come in handy to address the threat of the compromised forwarding nodes and since there are few, issues of congestions and delays in the network are avoided.

Motivation, Objective and Contribution: The following are the aims of the research:

Investigate wireless sensor networks security design issues and challenges and the various attacks that adversaries can launch via malicious nodes. Design and implement a prototype of an enhanced malicious node detection scheme by amalgamating the Weighted Trust Evaluation Scheme and Stop Transmit and Listen (STL) scheme. Evaluate malicious node detection and isolation by analyzing the response time, detection ratio, and the misdetection ratio of the above-proposed scheme. Malicious and faulty nodes in Wireless Sensor Networks can send falsified reports or erroneous data to the base station. This is catastrophic as mission-critical applications like military surveillance and health care WSN rely on accurate and timely data for reliable functioning of the network; for example, in a battlefield surveillance WSN a distorted misleading report pertaining the enemy operations may result to extra casualties. Ensuring that malicious nodes are detected and isolated as early as possible in the SWSN ensures accurate data is send leading to the right decisions being made. This would go a long way in ensuring that the border surveillance WSN is reliable and can be depended upon to alert the personnel manning the border of terrorists, illegal immigrants and smugglers crossing the borders at non-designated points. The study also adds to the body of
knowledge in the field of surveillance WSN. The envisioned malicious node detection and isolation scheme once deployed can be useful for further research in WSN malicious node detection.

II. LITERATURE REVIEW

This section analyses and reviews published work in the area of security of Wireless Sensor Networks (WSNs) and malicious node detection and isolation schemes. It commences with a brief introduction of WSN, an investigation on the major design challenges and issues in the WSNs security, the security goals of WSNs, attacks emanating from malicious nodes and then an analysis of malicious nodes detection schemes.

2.1. Why This Project?

Detection and isolation of malicious or malfunctioning nodes in border surveillance WSN is a major security issue. These nodes must be detected and excluded in the sensor network to avoid catastrophic decisions being made as a result of falsified information injected by the adversary as well as prevent an array of attacks that can emanate from malicious nodes. Attacks emanating from malicious nodes are the most dangerous attacks. These necessitate that their detection and isolation be given top priority as malicious nodes can send erroneous or falsified reports (Byzantine problem) to the base station leading to a disastrous decision; such as, in the battlefield surveillance WSN a misleading report about the enemy operations may result to extra casualties.

2.2. Surveillance Wireless Sensor Network

Surveillance Wireless Sensor Networks (SWSN) are deployed along the border or perimeter areas to monitor the real-world phenomena of interest in detail and detect unauthorized intrusions by hostile elements. The sensor nodes can either be deployed randomly via aerial deployment or deterministically where the exact locations of the sensor nodes are pre-determined. An SWSN can be employed in a broad range of places ranging from country borders for military surveillance, wildlife parks to monitor endangered animal species, embassies, and factories.

Once the sensor nodes are deployed to a region of interest; they organize themselves forming an operational sensor network and then start sensing the target area for intrusions such as tank vibrations, troop movements, or sniper gun noise. The sensed event is relayed to the sink node via the cluster heads (forwarding nodes). To lessen the communication overhead, forwarding nodes perform data
aggregation/compression on the sensed data before its transmission to the base station to provide situational awareness so that an appropriate action can be taken.

The main objective of border SWSN is the detection of enemy intrusions and alerting the military or the responsible personnel of targets of interest such as trespassers or moving vehicles in hostile environments or within a predefined area. Dense sensor nodes deployment is done in the border location to ensure robustness. Security is an essential requirement in SWSNs used in mission-critical tasks such as military surveillance. Sensor nodes can easily be compromised by the attacker due to constraints like limited sensor node energy, limited computation and communication capabilities, and the hostile deployment environments. The adversary may inject false data using the compromised nodes thus misleading the network operator; this has catastrophic consequences. In this research we investigate malicious node detection schemes with special interest in weighted trust evaluation scheme.

2.3. Challenges in Designing Wireless Sensor Network Security Schemes

The following are the various design issues and challenges within Wireless Sensor Network’s platform that make the employment of existing security mechanisms inadequate and inefficient

2.3.1) Very Limited Resources

The acute resource scarcity of sensor nodes poses significant challenges to resource-intensive security mechanisms. These mechanisms require certain amounts of resources such as energy, data memory and code space to function well but these resources are constrained in a tiny sensor node. The hardware constraints demand that the security algorithms used be extremely efficient in terms of memory, computational complexity, and bandwidth, (Padmavathi & Shanmugapriya, 2009).

Energy which is the most treasured resource for sensor networks also happens to be the biggest constraint as it limits its capabilities and must, therefore, be conserved or used effectively by the security mechanisms in place. Since the internal batteries of sensor nodes deployed in the field (hazardous environments) cannot be replaced or recharged easily; battery charge must be conserved as much as possible to extend the lifetime of the node and the sensor network in general. (SHARMA & TRIPATHI, April 2015). Communication is a power-intensive task and the security mechanisms used are required to be energy-efficient.

2.3.2) Unreliable Communication

Due to the inherent broadcast nature of the wireless communication medium employed in WSNs; packets may be distorted as a result of channel errors leading to conflicts, packets may also be dropped at highly congested nodes and an adversary can easily launch a Denial-of-Service (DoS) attack.

2.3.3) Unattended Operations

The sensor nodes may be left unguarded for a long period in the field; this though depends on the application function of the sensor network in consideration. There are three major cautions to these unattended sensor nodes (Padmavathi & Shanmugapriya, 2009):
Exposure to Physical Attacks: Sensor nodes may be deployed in a hostile environment exposed to adversaries and bad weather conditions. The probability that a sensor node suffers a physical attack like capture or destruction by an attacker in such an environment is therefore high.

Managed Remotely: Sensor network remote management makes it nearly impossible to detect physical node tampering and manipulation by the adversaries.

Lack of a Central Management Point: To increase sensor network vitality, a wireless sensor network needs to be a distributed network devoid of a central management point. However, an incorrect or poor design will make the sensor network organization inefficient, difficult, and fragile.

2.4) Security Goals for Wireless Sensor Networks
The main objectives of Wireless Sensor Networks (WSNs) security are as follows:

2.4.1) Data Confidentiality
Confidentiality refers to the ability to conceal vital messages' content from being disclosed to an unauthorized party or protect the messages against unintended access. Sensor nodes may exchange or pass highly sensitive information. Data authentication is therefore needed so that the receiving node can confirm that the data originates from the claimed sender (correct source).

2.4.4) Data Availability
Availability seeks to ensure that the required network services are functioning at a desired level of performance and work promptly in such as cryptographic key distribution and it must, therefore, remain confidential. This means that it is very crucial to build a secure communication channel in a sensor network. Data encryption should also be used to secure the data being transmitted across the sensor network.

2.4.2) Data Integrity
Data integrity is referred to as the ability to assert that the message was not altered, tampered with or improperly modified in transit by an adversary. It is essential to guarantee data reliability. The sensor network integrity will be compromised when (Padmavathi & Shanmugapriya, 2009):

- A malicious node in the network injects incorrect and misleading data.
- Unstable and turbulent conditions resulting from the wireless communication channel causing data damage or loss. (Akyildiz, et al., 2002)

2.4.3) Data Authenticity
Authentication ensures the reliability of the received message through source identity verification. An attacker can alter the data packet or even modify the whole packet stream by introducing extra bogus packets.

III. PROPOSED ARCHITECTURE
MATrix LABoratory (MATLAB) is a multi-paradigm tool for technical computing, data analysis and visualization, algorithm, and interactive development. It is both a computational and application development platform. MATLAB is well suited for performing computationally intensive tasks, solving mathematical problems, modeling, simulation, and control theory-related applications. Simulink is a block diagram environment fully integrated with MATLAB. It supports model-based design, simulation, automatic generation of code, testing, and verification of dynamic and embedded systems including image, signal and video processing, communications, and control systems. It also provides customizable block libraries and an interactive graphical environment. The customizable block libraries and the responsive graphical environment enable the users to perform design, simulation, implementation, and testing of a range of time-varying systems such as controls, communications, signal processing, image and video processing.

MATLAB offers the advantage of quick prototyping, fast computational engine, integration with other programming languages, and the ability to work with different data sources. Our research considers a wireless sensor network (WSN) with \( n \) sensor nodes randomly distributed in a region \( R \). A subset of the \( n \) nodes are powerful forwarding nodes. The nodes form clusters and the powerful nodes act as cluster heads/forwarding nodes forwarding data to the base station. Sensor nodes in close neighborhood (members of one cluster) register similar readings else they are deemed malevolent. Each node \( j \) collects data samples about its local environment and transmits the data to the forwarding node which acts as the intermediate to the base station. The communication path over which the sensed values are propagated from the source node \( j \) to the forwarding and then to the base station is assumed to be error-free so the data reaches the base station without modification en route. We also assume that the bandwidth of the wireless channel used in transmission is not limited so contention issues are reduced.
IV. SIMULATION RESULTS AND DISCUSSION

To carry out performance evaluation of the enhanced weighted trust evaluation scheme, the following evaluation specific objectives were set

- To find out the average number of cycles required to correctly detect malicious nodes present in the wireless sensor network.
- To find out the number of correctly detected malicious sensor nodes concerning the total number of malicious nodes in the sensor network under various simulation parameters.
- To find out the ratio of undetected sensor nodes to the total number of detections made by the scheme under the various simulation parameters.
- To show that the scheme has a short response time, high detection rate as well as a low misdetection ratio

1) Response Time

Response time (RT) refers to the average number of cycles required by the scheme to correctly detect malicious nodes in the sensor network. Response time is used to show how quickly the enhanced WTE based scheme detects malicious nodes present in a sensor network.

2) Detection Ratio

Detection Ratio (DR) refers to the ratio of malicious nodes detected by the scheme to the total number of malicious sensor nodes present in the WSN. It is used as a scheme effectiveness indicator. A high DR is key in ensuring misleading reports emanating from malicious sensor nodes present in the WSN are eliminated.

3) Misdetection Ratio

Misdetection ratio (MR) refers to the ratio of undetected nodes to the total number of all detections made by the scheme; this includes malicious nodes correctly detected and all undetected nodes. Misdetected nodes belong to two classes: malicious nodes considered normal as well as normal nodes considered malicious. The misdetection ratio of the scheme should be as low as possible to reduce false positives

V. CONCLUSION

The research project had several objectives set and was to be achieved throughout the project implementation. The objectives were; first, Investigate wireless sensor networks security design issues and challenges and the various attacks that adversaries can launch via malicious nodes. Secondly, design and implement a prototype of an enhanced malicious node detection scheme by amalgamating the Weighted Trust Evaluation Scheme and Stop Transmit and Listen (STL) scheme and thirdly evaluate malicious node detection and isolation by analyzing the response time, detection ratio.
and the misdetection ratio of the above-proposed scheme.

The research project delved into detailed wireless sensor network security design issues and challenges such as limited energy and computational capabilities, unreliable wireless communication medium, and the hostile deployment environment. These design issues and challenges render the employment of existing security mechanisms inadequate and inefficient. This coupled with the fact that owing to the constrained resources inherent in the sensor node, most wireless sensor network protocols tend to assume a high level of trust between the communicating sensor nodes to eliminate the authentication overhead creates the danger of adversaries introducing malicious nodes to the sensor network or manipulate existing ones and subsequently using them to propagate a wide range of attacks such as sinkhole attack, Sybil attack, black hole attacks, wormhole attack, HELLO flooding attacks and Denial-of-Service attacks. Detection and exclusion of such malicious nodes are crucial.

The second objective was met via the design and development of the scheme. An enhanced weighted trust evaluation scheme was designed using system model diagrams, control flow diagrams, flow charts and pseudo-codes to show how the algorithm works and to depict the flow of our algorithm's logic. The algorithm design was then developed and implemented using the MATLAB language. The MATLAB platform was chosen due to its advantage of quick prototyping and fast computational engine.

The third objective which involved testing and evaluating the performance of our scheme was also accomplished. The evaluation involved verifying that the initial model requirements specification has been met by the output of the implemented algorithm. The main features tested include the generation of short response timings, high detection rate, and low misdetection ratio. It was also demonstrated that the ratio of malicious nodes to the total number of sensor nodes in WSN affects the detection ratio of the scheme. Results obtained were plotted graphically and it was found out that the ratio of malicious nodes to the total nodes deployed directly affects the detection ratio in that as the number of malicious nodes in the network increases, the detection ratio decreases. The algorithm can be thus said to be suitable to detect malicious nodes in WSNs in which the ratio of malicious nodes to the total number of nodes is less than 0.5.

REFERENCES


