Malicious Node Detection in WSN

Reema[1], Shabnam Kumari[2], Pinkee[3]
[1,2] *A.P, Department of CSE, Sat Kabir Institute of Technology & Management, Bahadurgarh, Haryana, India*
[3] *M.Tech scholar, Dept of CSE, Sat Kabir Institute of Technology & Management, Bahadurgarh, Haryana, India*

***Abstract*- Wireless Sensor Networks (WSNs) present myriad application opportunities for several applications such as precision agriculture, environmental and habitat monitoring, traffic control, industrial process monitoring and control, home automation and mission-critical surveillance applications such as military surveillance, healthcare (elderly, home monitoring) applications, disaster relief and management, fire detection applications among others. Since WSNs are used in mission-critical tasks, security is an essential requirement. Sensor nodes can easily be compromised by an adversary due to unique constraints inherent in WSNs such as limited sensor node energy, limited computation and communication capabilities and the hostile deployment environments.**

***Index Terms*- WSN, WTE, STL, SWSN.**

1. INTRODUCTION

Wireless sensor network (WSN) consists of a large number of spatially distributed autonomous sensor nodes operating collaboratively to monitor the surrounding physical or environmental conditions (monitored target) and then communicate the gathered sensory data to the main central location through wireless links. A sensor node (mote) is a small, low-powered, wireless device, with limited computation and communication capabilities, 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. (Hussain, et al., April, 2013).

A sensor node comprises of a sensor, memory, processor, mobilizer, communication system, power units and position finding system. Each sensor node is made up of three subsystems namely:

- Sensor subsystem that senses the physical phenomena or environmental conditions.
- Processing subsystem that performs local computations operations on the sensed data.
- Communication subsystem that is responsible for message transmission and exchanges among neighboring sensors.

Sensors can monitor several phenomena such as humidity, temperature, lighting conditions, pressure, vehicular movement, noise level, chemical concentrations, soil makeup, and other properties. There are several types of sensors which include infrared, seismic, thermal, magnetic, acoustic, visual and radar based on the sensing mechanism employed by them (Ali , 2012).

Once the phenomena is sensed, the data collected (measurement) is converted into signals for further processing to reveal some characteristics pertaining the phenomenon from the target area (Hussain, et al., April, 2013)

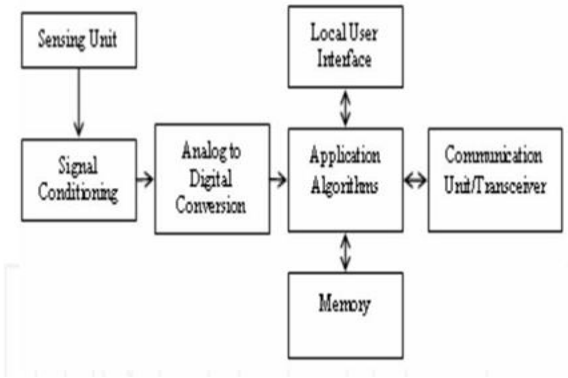

Figure 1: Sensor node basic architectural components (Ali , 2012)

WSN have great potential for deployment in mission-critical applications like battlefield surveillance applications, healthcare (elderly people, home-patient monitoring), disaster relief as well as fire detection applications among others. Since WSNs are

employed in mission-critical tasks, security is an essential requirement. However, sensor networks pose unique challenges and as such existing traditional security schemes used in traditional networks are inadequate (PERRIG, et al., June 2004). Limited sensor node energy, computation and communication capabilities and the hostile deployment environments bring a challenge of employing efficient security solutions in WSN.

1.1.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 by deployed randomly via aerial deployment or deterministically where the exact locations of the sensor nodes are pre-determined. A 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). In order 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. PROBLEM STATEMENT

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. In order 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 manipulate 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 is crucial that these nodes be detected and excluded in the sensor network to avoid 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 report (Byzantine problem) to the base station leading to a disastrous decision; such as, in a battlefield surveillance WSN a misleading report about the enemy operations may result to extra casualties.

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.

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 so as 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.

Clearly, security mechanisms employed in a sensor network must strive to be communication efficient in order to achieve energy usage minimization. Effective security mechanisms are also required to limit the security algorithm's size since the sensor node has limited memory and low storage capacity.

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.

The multi-hop routing, network congestion and node processing can result to greater latency in the sensor network resulting to synchronization issues among sensor nodes. These issues can hinder sensor network security especially where the security mechanism is based on cryptographic key distribution and critical event reports. (CHELLI, 2015)

3.3.Unattended Operations

The sensor nodes may be left unguarded for a long period of time 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: In order increase sensor network vitality, a wireless sensor network need 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.

3.4. Hostile Environments

Sensor nodes in extremely hostile deployment environments are susceptible to destruction or capture by the adversaries as they are exposed to them. Attackers can capture a sensor node, disassemble it, and extract valuable information such as cryptographic keys from it.

4. SECURITY GOALS FOR WIRELESS SENSOR NETWORKS

The main objectives of Wireless Sensor Networks (WSNs) security are as follows:

4.1. Data Confidentiality

Confidentiality refers to the ability to conceal vital messages' content from being disclosed to unauthorized party or protect the messages against unintended access. Sensor nodes may exchange or pass highly sensitive information 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.

4.2. Data Integrity

Data integrity is referred 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. (Akykildiz, et al., 2002)

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. Data authentication is therefore needed so that the recipient node can confirm that the data actually originates from the claimed sender (correct source).

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 normal situations as well as in the event of attacks or environmental mishaps. It implies that the sensor node has the ability to access and utilize the available resources and that the network is operational and ready for use to transmit messages.

4.5. Data Freshness
This ensures that the transmitted messages are current and old content (expired packets) are not replayed by an adversary to either mislead the network or keep the network resources busy thereby reducing the sensor network vitality. It is essential especially in shared-key design strategies that require the keys be changed over time. (CHELLI, 2015)

4.6. Secure Localization
Sensors may get displaced during their deployment, after a certain length of time or after a critical displacement incident. WSN operations depends on its ability to automatically and accurately locate each sensor node in the network after the displacement. (CHELLI, 2015).

4.7. Self-Organization
WSN being an ad-hoc network and lacking a fixed infrastructure for network management requires that each node be independent and versatile so as to be able to self-organize and self-heal depending on the various situations, topology and deployment strategy. This inherent feature of the sensor network is a great challenge to WSN security. If self-organization is absent in a wireless sensor network, an attack or the risky deployment environment may have dire consequences. (Padmavathi & Shanmugapriya, 2009)

4.8. Time Synchronization
Time synchronization is required by many WSN applications, it is essential in multi-hop communication, conservation of node energy (periodic time sleep) and node localization. Sensor nodes may wish to determine the network latency of a packet as it transits between a pair of sensor nodes (sender-receiver) (Padmavathi & Shanmugapriya, 2009). Collaborative time synchronization may be needed by wireless sensor network for tracking applications.

5. MALICIOUS NODES DETECTION TECHNIQUES

Several schemes for malicious node detection and isolation in WSNs have been proposed.
(Sung & Choi, 2013) Proposed a Dual Threshold technique for malicious node detection that employs two thresholds to minimize false alarm rate as well as improve the detection accuracy. All deployed sensor nodes do have transmission ranges, 'tr', and any other sensor node in close proximity i.e. within the node transmission range is considered its neighbor. Each individual sensor node maintains its neighbors' trust values to designate their trustworthiness. The sensor node makes a localized decision based on its own readings and those of its neighbors taking into account their trust values. Trust values lie between 0 and 1. If Tik=0 means node Ni does not trust Nk at all. A node also has its own trust value, once Tii=0 means the node is faulty.
(Curiac, et al., 2007) Proposed Auto regression Technique which is a mechanism that relies on past/present sensor node values. The sensor node present value is compared with an estimated value computed from its own previous values by an

autoregressive predictor placed at the base station. The two values are compared to check if node behavior is normal or abnormal. If the variance between these two values is higher than a set threshold, the node is regarded malicious.

(Yang, et al., 2007) Proposed SoftWare-based ATTestation (SWATT) mechanism to authenticate the embedded device (sensor nodes) memory contents and detect any falsification or maliciously altered or inserted code in memory. The verifier send to the embedded device a randomly generated MAC key, which then calculates Message Authentication Code (MAC) value on the whole memory using the received key and returns the MAC value. The verifier uses the checksum to verify the memory contents. If the memory has been maliciously altered by the adversary then the checksum is false.

(Bao, et al., 2011) Proposed a Trust-Based Intrusion Detection approach which considers a composite trust metric derived from both social trust and quality of service (QoS) trust to identify malicious nodes in the wireless sensor network. The cluster head apply intrusion detection in the sensor nodes to assess the trust worthiness and maliciousness of the nodes in its cluster. This is achieved by statistically examining peer-to-peer trust evaluation results gathered from the different sensor nodes (Sumathi & Venkatesan, 2014).

(Nidharshini & Janani, December 2012.) Proposed a Sequential Probability Ratio Testing (SPRT) to detect duplicate nodes made by an adversary in the WSN. The attacker can easily capture and make replicas of unattended nodes and then use them to take control of the entire network. The base station is responsible for identifying compromised nodes by computing the speed of observed sample nodes and decides which nodes' speed exceeds the decided threshold speed, these ones are regarded malicious.

5.1. Weighted Trust Evaluation Scheme.

Weighted-Trust Evaluation (WTE) based scheme is a light-weighted algorithm used to detect and subsequently isolate compromised (malicious) nodes by monitoring their reported data in a hierarchical WSN architecture. (Zhao, et al., March 2013) (Atakli, et al., 2008) Employed and demonstrated this method using a three-layer hierarchical sensor network. The components of the three-layer hierarchical network architecture are:

a) Low-power Sensor Nodes (SN) whose functionalities are limited. SN is in the lowest tier and does not offer multi-hop routing capacity as in a traditional flat sensor network. SNs report the data to its Forwarding Node.
b) Higher-power Forwarding Nodes (FN) which collect data from the lower layer (SNs), verify its correctness, aggregate and forward it to other FNs or to the upper layer (Base Station).
c) Base Stations (BS) or Access Points (AP) which verifies data reported by the FNs as well as routing data between the wireless sensor network and the wired infrastructure.

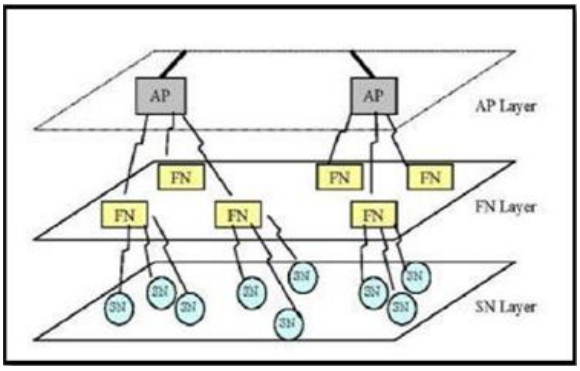

Figure 5: Architecture of the hierarchical WSN (Atakli, et al., 2008).

This scheme is based on two assumptions; first, the FNs and Base station are trusted nodes that cannot be compromised by an attacker since once an adversary seize control of the BS then they can launch any possible attack in the sensor network (Sumathi & Venkatesan, 2014) (Hu, et al., 2009) (Atakli, et al., 2008). Another critical assumption is that the normal nodes (working in proper condition) in the sensor network exceeds in number the compromised nodes. Otherwise, the scheme may misidentify normal node as compromised nodes increasing false positives. The proposed enhanced WTE intends to detect and isolate malicious FNs in the sensor network instead of assuming they won't be compromised by adversaries. This aims to cautions all the SNs under a FN which the attacker can control and manipulate once it take control of a particular FN.

5.1.1. Malicious Nodes Detection

A compromised sensor node provides falsified information that may wrongly mislead the senor network. This problem is referred as the Byzantine problem. A compromised/malicious sensor node can

continuously forward wrong information to the upper layers. The aggregator (AP or FN) in the upper layer may compute an incorrect aggregation result due to the misleading information emanating from the malicious nodes. This may have disastrous effects to the decision making process.

WTE scheme models malicious node detection and isolation in 2 steps;

First, an initial weight Wn is assigned to every sensor node (SN) in the sensor network. The Forwarding Node (FN) gathers all the reported data from all the SNs under it and computes an aggregated result taking into account each SN weight.

$E = \sum_{=1} / \sum_{=1}$

Where: E = FN aggregate result.

Wn =SN assigned weight (Ranging between 0 and 1).

Un = SN output information (Un is usually dependent on the sensor network application. The output value may be "true" or "false" or continuous numbers like in a case of temperature readings).

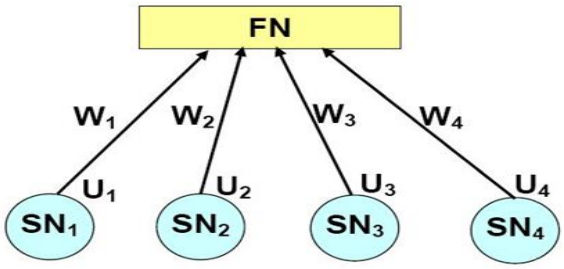

Figure 6: Weight-based hierarchical wireless sensor network (Atakli, et al., 2008).

Each SN weight is updated based on the accuracy of the reported information. The SN weight is updated for two reasons. First, if a compromised sensor node continuously forward data that is inconsistent with the final aggregate decision, its weight is likely to be reduced by a set weight penalty. If the weight decreases below a given threshold, then it is identified as a malicious node. Second, the SN weight determines how much a sensor node report contributes to the final aggregate decision. This is meant to lower the effect of incorrect reports from malicious sensor node.

5.1.2. Weight Value Recovery

The SN weight is decreased by a certain penalty value once it is detected to be reporting falsified data. However, the false report may be a result of a temporary communication channel interruption and the SN is neither malicious nor faulty. The weight values for such SNs needs to be recovered after the disturbance rather than keeping these values low permanently. The SNs that behave correctly thereafter longer than a set recovery time have their weight value increased.

5.2 Stop Transmit and Listen (STL)

The STL scheme employs non-transmission time slots to detect malicious nodes. Each sensor node have an inbuilt time limit to stop their data transmissions and listen for traffic. Once the nodes have been deployed and they have started sensing the target phenomena, the sensed data is sent to the base station. After every few seconds or after a set transmission time, each sensor node halt their data transmission process and listens for malicious traffic. If a sensor node transmits data during the non-transmission time (listening time) , it is caught by its neighbor nodes in the sensor network and it is regarded malicious as it exhibits malicious behavior. If a malicious node doesn't transmit data during a non-transmission time slot, it will still be caught in other frequent non-transmission times. The malevolent behavior of a malicious node is broadcasted across the entire sensor network. (Sathyamoorthi,et al., 2014). Then every other sensor network node desist from either forwarding data to the detected malicious node or accepting from it.

This technique has some weaknesses such that when the whole network or a major portion of it stopped their transmission at a time (during non-transmitting time) and then resume transmission, congestion and unwanted delay in the network operations arises (Sumathi & Venkatesan, 2014).

6. CONCLUSION

The research paper 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 so as 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 is crucial.

REFERENCES

[1] Alam, D. S. & Debashis, 2014. ANALYSIS OF SECURITY THREATS IN WIRELESS SENSOR NETWORK. International Journal of Wireless & Mobile Networks (IJWMN), Volume 6.

[2] Ali, Q. I., 2012. Simulation Framework of Wireless Sensor Network (WSN) Using MATLAB/SIMULINK Software. In: s.l.:s.n., pp. 263-264.

[3] Das, R., Purkayastha, D. B. S. & Das, D. P., 2002. Security Measures for Black Hole Attack in MANET: An Approach. Proceedings of Communications and Computer.

[4] Karuppiah, A. B. & Rajaram, S., 2014.. False Misbehavior Elimination of Packet Dropping Attackers during Military Surveillance using WSN. Advances in Military Technology, 9(1).

[5] Abdullah, M. I., Rahman, M. M. & Roy, M. C., 2015. Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count. I. J. Computer Network and Information Security, p. 51.

[6] Akykildiz,. I. F., Su, W., Sankarasubramaniam, Y. & Cayirci, E., 2002. A Survey on Sensor Networks. IEEE Communication Magazine.

[7] Alajmi, N., July 2014. Wireless Sensor Networks Attacks and Solutions. International Journal of Computer Science and Information Security (IJCSIS) , 12(7).

[8] Atakli, I. M. et al., 2008. Malicious Node Detection in Wireless Sensor Networks. The Symposium on Simulation of Systems Security (SSSS'08), Ottawa, Canada, p. 838.

[9] Bao, F., Chen, I.-R., Chang, M. & Cho, J.-H., 2011. Trust-Based Intrusion Detection in Wireless Sensor Networks. Kyoto, Japan, s.n.

[10] Cannon, B. J., May 2016. Terrorists, Geopolitics and Kenya's Proposed Border Wall with Somalia. Journal of Terrorism Research, 7(2), pp. 27-28.

[11] CHELLI, K., 2015. Security Issues in Wireless Sensor Networks:Attacks and Countermeasures.

[12] Proceedings of the World Congress on Engineering 2015, Volume 1, pp. 1-6.

[13] Curiac, D.-I.et al., 2007. Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique. Athens, Greece, s.n.

[14] Hu, H. et al., 2009. Weighted trust evaluation-based malicious node detection for wireless sensor networks. Int. J. Information and Computer Security, 3(2), p. 148.

[15] Hu, Y.-C., Perrig, A. & Johnson, D. B., 2003. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. s.l., s.n.

[16] López, E. E. et al., 2005. Simulation Tools for Wireless Sensor Networks. Cartagena, Spain., s.n., pp. 5-9.

[17] Nayyar, A. & Singh, R., 2015. A Comprehensive Review of Simulation Tools for Wireless Sensor Networks (WSNs). Journal of Wireless Networking and Communications, Issue 2167-7328, pp. 110-113.

[18] Pathan, A.-S. K., 2010. DENIAL OF SERVICE IN WIRELESS SENSOR NETWORKS: ISSUES AND CHALLENGES. In: Advances in Communications and Media Research. s.l.: Nova Science Publishers, Inc..

[19] PERRIG, A., STANKOVIC, J. & WAGNER, D., June 2004. SECURITY IN WIRELESS SENSOR NETWORKS. COMMUNICATIONS OF THE ACM, 47(6).

[20] Sathyamoorthi, T., Vijayachakaravarthy, D., Divya, R. & Nandhini, M., 2014. A SIMPLE AND EFFECTIVE SCHEME TO FIND MALICIOUS NODE IN WIRELESS SENSOR NETWORK. International Journal of Research in Engineering and Technology, 03(02).