International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Malicious Node Detection in WSN Using WTE

Rashmi[1], Sumit Dalal[2], Shabnam Kumari[3]
[1]M.Tech. Scholar, Department of ECE
[2]Assistant Professor, Department of ECE, [3]Assistant Professor, Department of CSE
[1,2,3]SKITM, Bahadurgarh, Haryana, India

ABSTRACT
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. These unique challenges render existing traditional security schemes used in traditional networks inadequate and inefficient. An adversary may take control of some sensor nodes and use them to inject false data with the aim of misleading the network's operator (Byzantine attack). It is therefore critical to detect and isolate malicious nodes so as to prevent attacks that can be launched from these nodes and more importantly avoid being misled by falsified information introduced by the adversary via them. This research gives emphasis on improving Weighted Trust Evaluation (WTE) as a technique for detecting and isolating the malicious nodes. Extensive simulation is performed using MAT LAB in which the results show the proposed WTE based algorithm has the ability to detect and isolate malicious nodes, both the malicious sensor nodes and the malicious cluster heads (forwarding nodes) in WSNs at a reasonable detection rate and short response time whilst achieving good scalability.

Keywords: *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.

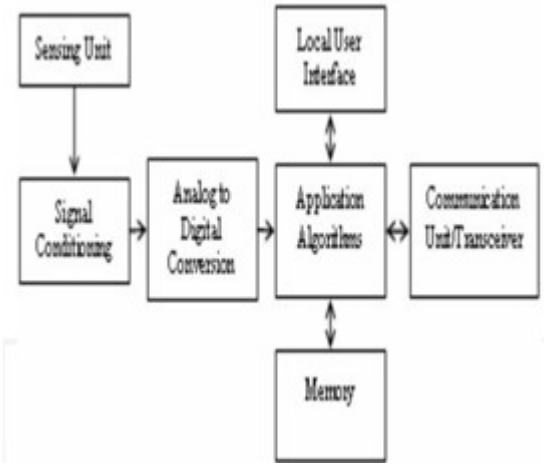

Figure 1: Sensor node basic architectural components (Ali , 2012)

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. 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 manipulates existing ones and then subsequently uses 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

2. OBJECTIVES:

The following are the aims of the research:

1) Investigate wireless sensor networks security design issues and challenges and the various attacks that adversaries can launch via malicious nodes.
2) 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

3. CONCEPTUAL FRAMEWORK:

The research evaluates the performance of the enhanced WTE for detection and isolation of malicious node in WSN via three identified metrics namely response time, detection rate and misdetection ratio. Response time is used to show how quick the enhanced WTE based scheme detects malicious nodes present in a sensor network. It is the average number of cycles required by the scheme to correctly detect malicious nodes. A short response time that ensures malicious nodes are isolated as early as possible in the WSN is desirable so as to lessen the disastrous effects of these nodes on the overall operation of the sensor network.

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. Detection ratio is used to indicate the effectiveness of our enhanced WTE scheme. The DR should be high to ensure that all malicious nodes are detected and isolated in the sensor network. This is key in eliminating misleading report emanating from malicious sensor nodes present in the WSN.

The third metric is Misdetection ratio, which refers to the ratio of misdetected nodes to the total number of all detections made by the scheme; this includes malicious nodes correctly detected and all misdetected nodes. Misdetected nodes belong to two classes: malicious nodes considered normal by the scheme and normal nodes considered malicious. The misdetection ratio of the scheme should be as low as possible so as to reduce the false positives reported.

The aim entailed designing and developing a sensor network malicious node detection scheme with high

detection rate, short response time and low misdetection ratio.

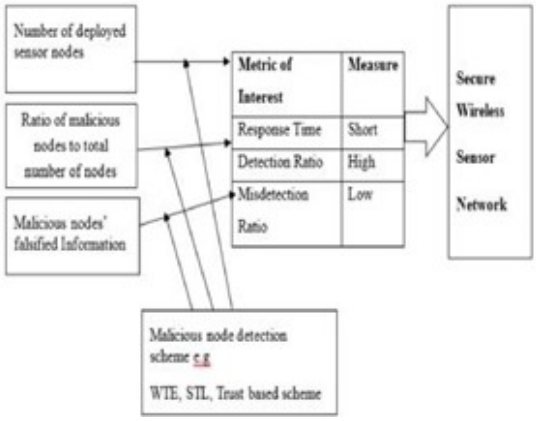

Figure3.1. Conceptual Framework

The ratio of malicious nodes present in the network to the total number of deployed sensor nodes affects the detection and misdetection ratios in that when malicious nodes are the majority compared to the normal nodes, the number of misdetected nodes increases. Malicious nodes inject falsified data to mislead the sensor network.

4. ENHANCED WEIGHTED TRUST EVALUATION SCHEME.

A heterogeneous wireless sensor network made up of sensor nodes with different energy levels and processing power is assumed. The deployed sensor nodes are assumed to form two sets in the ratio of p: 1-p where p is the percentage of higher energy sensor nodes. The higher energy (powerful) subset is elected as the forwarding nodes (cluster heads). The forwarding nodes broadcast its presence to all the normal sensor nodes. Normal sensor nodes choose the cluster to belong based on the broadcasted signal strength. It is assumed that the stronger the signal, the closer the forwarding node. The normal sensor node ends up choosing the forwarding node with the shortest distance from it as its cluster head.

All the cluster sensor nodes members forward their sensed data to the forwarding nodes whereas the forwarding nodes forward the aggregated value to the sink node for further processing and decision making.

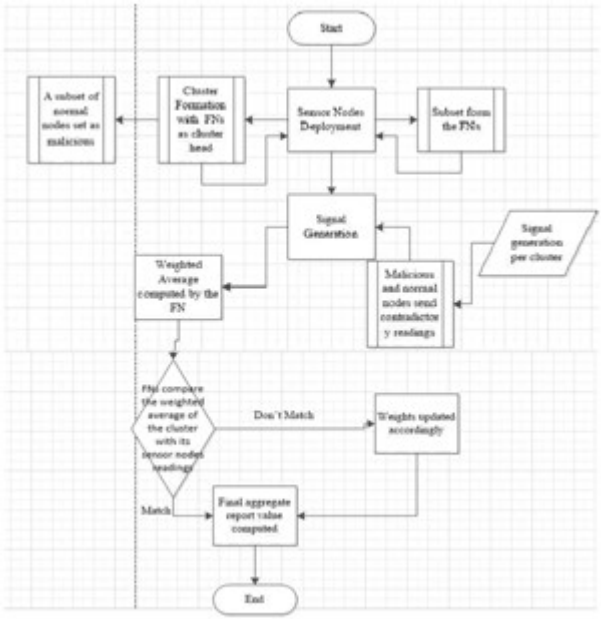

Figure 4.1: Enhanced Weighted Trust Evaluation Scheme - Control Flow Diagram.

4.1 Enhanced Weighted Trust Evaluation Algorithm

The algorithm comprises of two phases:

4.1.1 Deployment and selection phase

Step 1 : n sensor nodes deployed.
Step 2 : Select a subset (p) of the deployed nodes as the powerful forwarding nodes.
Step 3 : The forwarding nodes broadcasts a hello message (an advertisement message) to all normal sensor nodes.
Step 4 : The normal sensor nodes that have selected a particular forwarding node as their cluster head send an acknowledgement message to it and they become cluster members.

Normal sensor nodes decide on the cluster to belong based on its proximity to the cluster head since it is assumed that the nearest forwarding node (FN) broadcasted the strongest signal.

4.1.2 Data computation and transmission phase

Step 1 : Cluster member(s) transmit sensed data to the forwarding node (FN).
Step 2 : FN gathers the data forwarded by the normal sensor nodes under it.
Step 3 : FN perform an aggregation of the data collected taking into account the weights assigned to the normal sensor nodes.
Step 4 : The aggregate value is compared to the individual values of the normal sensor nodes.
Step 5 : The weights of the cluster members whose values are not in sync with the aggregate value are

gradually reduced till their values is below the minimum weight threshold set.

Step 6 : When the sensor node weight is below the minimum weight threshold, they are detected as malicious and isolated from the sensor network.

Step 7 : The forwarding nodes forward the aggregate data value to the base station

Step 8 : The forwarding nodes stop transmitting and listen for malicious traffic in the network during the non-transmission times.

Step 9 : The forwarding nodes transmitting during non-transmission times are detected as malicious.

The normal forwarding nodes only the send data to the base station during the transmission times. During the non-transmission times, they listen for any malicious traffic and are caught transmitting during these time slots are identified as malicious.

5. MALICIOUS SENSOR NODE MODELING

We consider a border monitoring WSN where the field or region is filled with IR (Infrared) sensors to detect any human presence. The region where the human presence is actually sensed is called an 'event region' whereas the other region is known as 'non-event region'. In case of human intrusion, the normal nodes in an event region send '1' directly to the FN indicating alarm. The other nodes (malicious nodes) send no alarm i.e. '0' to the FN. The malicious nodes in the non-event region send 1 (alarm) to the FN and the normal ones send a 0 (no alarm).

Let's consider each sensor node 'nj' in the network field reporting reading 'rj' such that rj= 1 for an event condition and 0 for no event condition. The aggregated value (E) gives the weighted average of the signal sensed by the deployed sensor nodes. If a sensor node is compromised by the adversary, it will send incorrect data to the FN making it transmit wrong data to the base station enabling the attackers achieve their aim of misleading the sensor network operator.

This malicious node detection algorithm is illustrated below:

1) Each sensor node nj sends a reading, rj to the Forwarding Node (FN). The normal sensor nodes send 1 (alarm) whereas the malicious ones send a 0 in case of an event and vice versa.
2) Each FN computes the aggregate value, E:

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

Where Wn= Weight assigned to the node

3) Each FN computes the percentage of nodes (Pe) that have reported an event and those that didn't (Pn). Aimed at achieving majority voting in a cluster.
   Pe = No. of nodes that reported an event/ Total number of nodes
   Pn = No. of nodes that did not reported an event/ Total number of nodes
4) If Pe >= Tu (upper threshold) then majority of the nodes sent an alarm signal, an event has occurred and the weights are updated accordingly.
5) If Pn <= Tl; Tl being lower threshold, then an event hasn't occurred and the weights are updated accordingly.
6) For steps 5 and 6 the interchange of the percentages Pn >= Tu and Pe <= Tl also applies
7) Determine the nodes with Wn = 0 as malicious.

The weight of the sensor node is gradually reduced by the penalty factor if it sends reading not in sync with the aggregate value of the forwarding node. The weight assigned to a node is updated to Wn = 0 if its weight is reduced below the set minimum weight threshold.

6. CONCLUSION

The issue of false positives in some clusters where compromised nodes outnumber the legitimate nodes. In such cases, the normal nodes were treated as malicious and malicious ones treated as normal. This leads to an increase in misdetection ratio.

The assumptions made include:

1) The access point (sink) is cannot be compromised by an adversary otherwise the attacker can launch any possible attack against the WSN upon taking control of the access point (AP).
2) The communication path over which the sensed values are propagated from the source sensor to the forwarding node and then to the base station is considered to be error-free so the data reaches to the base station without modification enroute.

The bandwidth of the wireless channel used in transmission is not limited so contention issues are reduced.

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
21. MALICIOUS NODE IN WIRELESS SENSOR NETWORK. *International Journal of Research in Engineering and Technology,* 03(02).