ISSN 2394-840X

Volume1, Issue 2, 15 February- 15 May 2015

International Journal In Applied Studies And Production Management

Design of IDS for Malicious Node Detection and Removal In WSN

Jaskirat Singh
Research Student, Dept. of Computer Science, Punjabi University, Patiala, India.

Dr. Rajneesh Randhawa
Assistant Professor, Dept. of Computer Science Punjabi University, Patiala, India

Abstract

WSN was developed for military and disaster rescue purposes only but because of the availability of ISM band (2.4 GHz), the technology is now growing rapidly in public applications. A wireless sensor network (WSN) consists of battery-operated sensor devices with computing, data processing, and communicating components. The WSN must be able to robustly detect such node outage and should be able to act quickly and efficiently in determining alternative routes to achieve reliable end-to-end communication between communicating nodes in the network

Key words: Nodes, WSN, Entity.

Introduction

Due to the recent advancement in wireless communication like Bluetooth, IEEE 802.11, or MANETs, a new concept of networking has emerged known as Wireless Sensor Networks (WSN). Wireless Sensor Network, consists of large number of sensor nodes. These nodes has the capability of wireless communication, limited computation and sensing. At first, WSN was developed for military and disaster rescue purposes only but because of the availability of ISM band (2.4 GHz), the technology is now growing rapidly in public applications. A wireless sensor network (WSN) consists of battery-operated sensor devices with computing, data processing, and communicating components. Wireless Networks provide a promising network infrastructure for many applications [1]. These technologies led to the implementation of wireless sensor networks, allowing easily configured, adaptable sensors to be placed almost anywhere, and their observations similarly transported over large distances via wireless networks.

Security and Attacks in WSN

Security in WSN is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. Security is critical for many sensor network applications, such as military target tracking and security monitoring.

Eavesdropping or passive information gathering

The communication medium of WSN applications is an unsecure wireless channel. An adversary, present in the region, may be able to intercept the communication between two legitimate nodes passively if the information is exchanged in plaintext. The adversary may monitor the communication which can later be used to carry out more sophisticated attacks against the WSN [2].

Node malfunctioning

A legitimate sensor node may at some point work inefficiently in the network. Malfunctioning of the sensor node may include dropping data packets at a high rate, denying packet forwarding requests (if working as a relay device), and soon. Such nodes need immediate detection as these conditions may severely affect the overall network performance [3].

Message’s injection

This active attack is to send many messages on the network. The aim of the attacker is to send false information [3].

Node outage

Some sensor nodes may work as relaying devices or routers in a WSN. A legitimate sensor node or router might stop functioning due to many reasons, as a result of which communication may fail among parts of the WSN [4]. The WSN must be able to robustly detect such node outage and should be able to act quickly and efficiently in determining alternative routes to achieve reliable end-to-end communication between communicating nodes in the network

.

Message corruption

An intruder may be able to join the network and impersonate legitimate relaying node between two communicating trusted entities [5]. Message integrity in this case may be attacked as the intruder may then be able to corrupt or modify the actual message contents resulting in a message corruption attack.

False node

An adversary may be able to add a sensor node to the network to misguide true nodes, exchange bogus data or corrupted data, block routes, and so on. This may lead to a communication bottleneck, false location claims, decrease in network performance, and so on [5]. This is an extremely dangerous attack which may lead to severe network damage or even annihilation.

Denial of Service (DoS)

DoS attack has various forms. Such an attack not only target disruption or interruption in network communication, but may also be used to temporarily weaken network capabilities to provide a service [5-6]. Blackhole, resource exhaustion, sinkhole, wormholes, flooding, induced routing loops, and so on are different types of DoS.

Node replication

An adversary may add a malicious node in the network by copying the identity of a true existing sensor node. This node may further bring severe damage to a WSN in various ways, including message corruption, injection of bogus data, misrouting information packets, and so on. Never the less, physical access to the network may compromise network secrets, security solutions, and so on. In security-sensitive applications of WSNs, the physical location information of a sensor node should not be disclosed to any unauthorized entity. Leakage of location information of sensor node may result in node compromiser node capture [6].

Jamming Attack

Jamming interferes with radio frequencies being used by the sensor nodes [6]. It could be powerful enough to disrupt the whole network or less powerful to disrupt a portion of this network. The problem to this attack is blacklisting of the adversary node.

Tampering

In this physical harm is made to a particular affected node [7]. The node is compromised or tampered by an attacker who makes a physical access to the node. The attacker gaining physical access to the node can extract extremely useful data such as the cryptographic keys etc. The solution to this attack is protection, tamper-proofing and changing of keys.

Selective forwarding

Multi-hop networks are often based on the assumption that participating nodes will faithfully forward receive messages. In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. The Black hole attack is a specific form of this attack in which a node drops all messages it receives. A solution is to identify the malicious node and assume that it has failed and take an alternative route [7-8].

Exhaustion

Attacker may violate the communication protocol and frequently send messages. This results in collisions which would in turn lead to retransmission of data. Repeated collisions thus lead to resource exhaustion [9]. Time-division multiplexing (TDM) could provide a solution to this problem. Another solution would be applying rate limitation at which data should be sent across a communication channel.

Collision

It occurs when two nodes simultaneously attempts to transmit data on the same frequency [10]. When packets collide, there are chances of a portion of data getting changed. This will cause an erroneous data transmission through a communication channel. The prescribed solution in the text is usage of error-correcting codes like CRC (Cyclic Redundancy Code).

Route information manipulation

This means changing the data being sent on a communication channel. To prevent this proper authentication mechanism can be used to identify the intended receiver. Also, encryption technique can be used to render the actual text unreadable, so that an eavesdropper is not able to intercept this text [10].

Sybil attack

In this attack, one node presents multiple identities to a network i.e. a single node duplicates itself and is presented in multiple locations [11]. Authentication techniques can be useful in preventing this attack.

Wormhole attack

In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them into the network [12].

Hello Flood attack

The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker [12].

Flooding attack

An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit [12]. In either case, further legitimate requests will be ignored. The solution involves limiting connection numbers.

Intrusion Detection System

It is a system that checks the behavior of the network to find out which node is not working normally [13]. This unit is installed on the client or on the server or on both the ends. It basically has a life cycle of three phases shown below:

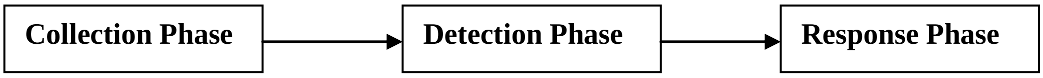


Figure 2.8.1 General structure of the IDS

The collection phase collects the network's data. Detection phase finds intrusion by applying a suitable detection policy. In case of abnormal activities, an alarm is generated by the response phase.

Intrusion Detection Model for WSN

(1) **Rule-Based IDS:** It is also known as Signature-based IDS. Rules based upon specific attacks have been articulated in such type of IDS model. So, sub-phases for these systems include the data acquisition phase, rule application phase and the intrusion detection phase [13].

(2) **Cluster-Based IDS:** This approach improves the security of clusters for sensor network. It primarily follows two approaches: model-based on authentication to resist external attacks; second model is based on an energy-saving mechanism which focuses on misbehavior both in the member nodes and the cluster-head nodes [14].

(3) **Hybrid IDS:** Both the cluster-based and rule-based IDS combines to form a hybrid IDS. This achieves the aims of high security and low energy consumption [15].

Comparison of IDS Models in Tabular Format

IDS Model	Network Architecture	Handled Attacks	Energy Consumption	Advantage	Disadvantage
Rule-Based	Distributed	DoS attacks, Sinkhole, Flooding, Blackhole, Selective forwarding.	Low	Detects all those attacks having specific rules, signatures.	Cannot detect new attacks.

Cluster-based IDS	Hierarchical		Low	Guaranteed data-delivery.	Increased traffic.
Hybrid IDS	Hierarchical	Selective forwarding, Sinkhole, Hello-flood and wormhole attacks.	Medium	Can detect both existing and new attacks.	Requires more computation and resources.

IDS Based Attack Detection and Removal

Rule-Based IDS for Flooding Attack

Rule 1: If the node A send a packet to node B than it stores the packet in its buffer and watch whether B has the capacity to forwards it or not. If B doesn't forward the packet or in any case drops the packet, then counter is not incremented by one and would hence increase the failure count. If the failure count is more than the threshold value, an alarm will be raised. In case of flooding attack, the packet drop count will be increased to a larger value as compared to that of the sinkhole attack.

Rule 2: If the majority of the monitor nodes have raised an alert then the target node is compromised and should be revoked or should be notified by the base station. Based on their rules, they have proposed an IDS block that is implemented in all the sensor nodes.

Rule-Based IDS for Sinkhole Attack

Rule 1: If the node A send a packet to node B than it stores the packet in its buffer and watch whether B forwards it or not. If B doesn't forward the packet, then counter is not incremented by one and would hence increase the failure count. If the failure count is more than the threshold value, an alarm will be raised.

Rule 2: If the majority of the monitor nodes have raised an alert then the target node is compromised and should be revoked or should be notified by the base station. Based on their rules, they have proposed an IDS block that is implemented in all the sensor nodes.

Proposed Intrusion Detection System

Proposed IDS agent in each sensor node consists of following modules:

- Local reply module
- Detection engine (Cooperative and Local)
- Communication
- Local packet monitoring

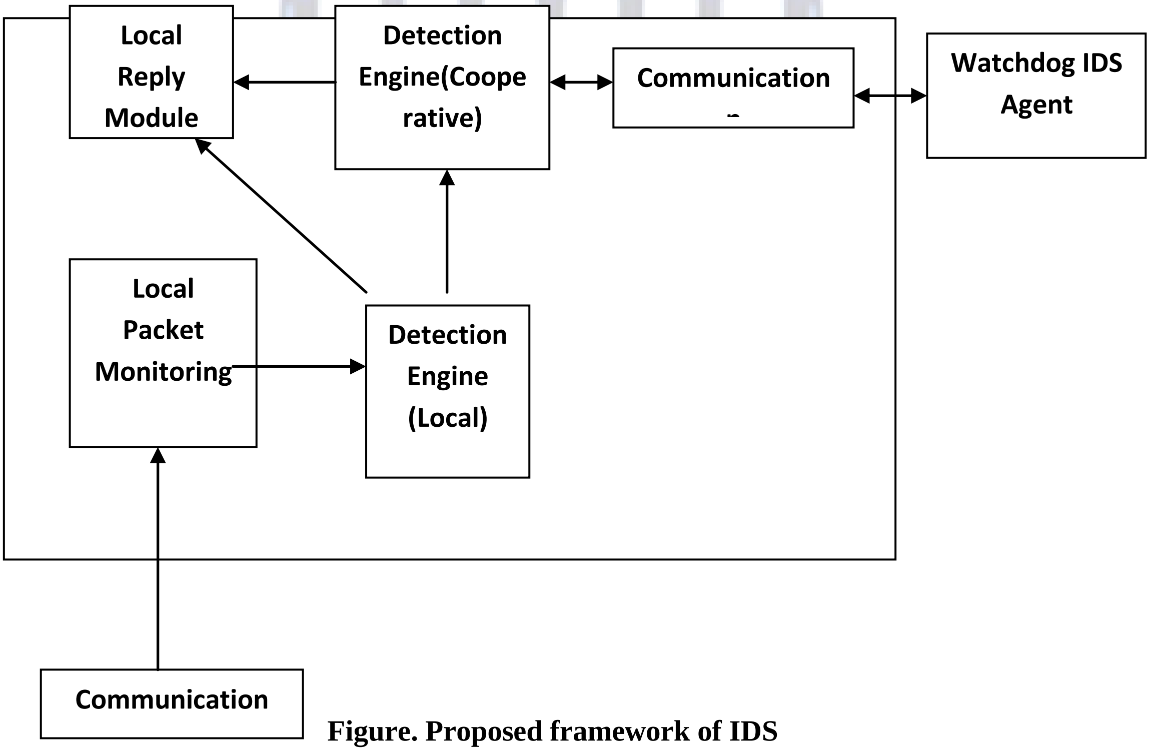
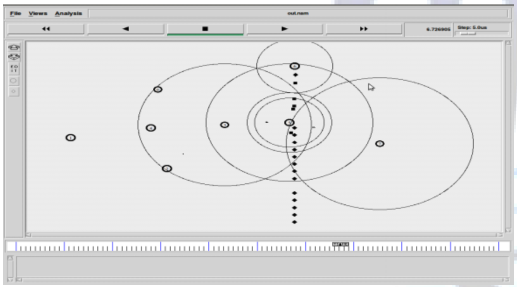


Figure. Proposed framework of IDS

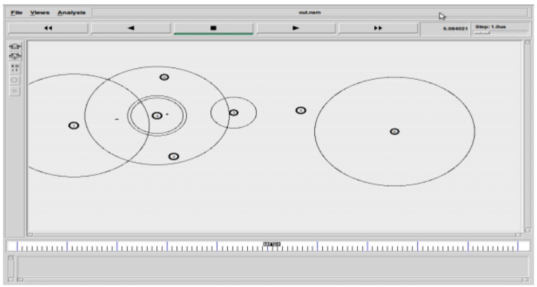
Local reply module sends the response to the base station, if any anomaly is found. In detection engine (cooperative) phase, if any of the node detects the intrusion then it shares information with the other nodes to minimize the false alarm rates. However, the local packet monitoring phase monitors the packet and also sends the data to the detection engine phase to detect the intrusion to detect the anomaly based on their unexpected behavior. Watchdog IDS agent uses local information of the next hop node and overhears it. If it gets that it spending time of the packet is exceeded above the predefined threshold then it marks that node as malicious, this way Watchdog approach detects malicious node in the network.

In our proposed research work, **Rule-Based IDS** have been applied for the detection of various attacks. It is host based in which every node has IDS. The architecture of the proposed IDS has many modules such as packet monitoring, cooperative engine, detection engine, and response unit. The IDS is basically designed for routing attacks and is capable of detecting packet-dropping attacks.

Scanerio for Flooding Attack :



With Attack



After Attack removal

ISSN 2394-840X

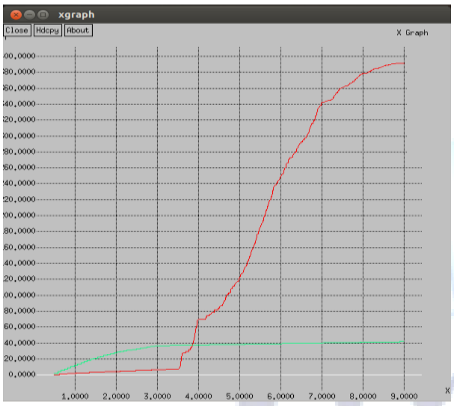
Volume1, Issue 2, 15 February- 15 May 2015

International Journal In Applied Studies And Production Management

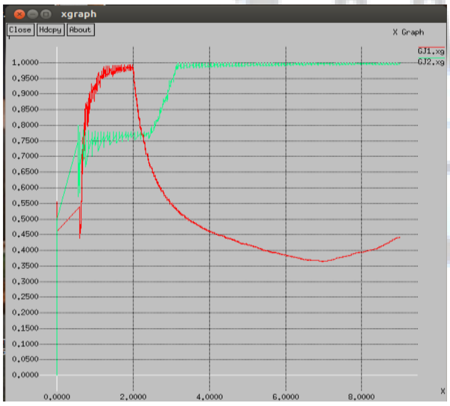
Performance Evaluation :

Red line shows with malicious node and Green line depicts the absence of malicious node.

1. **Delay :** It is the average time taken by data packets to reach the destination is known as delay or delay time.
2. **Packet Delivery Fraction :** Ratio of the number of packets received at destination to the number of packets sent from source.

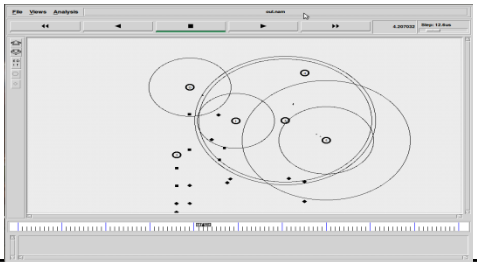


Delay Vs Time

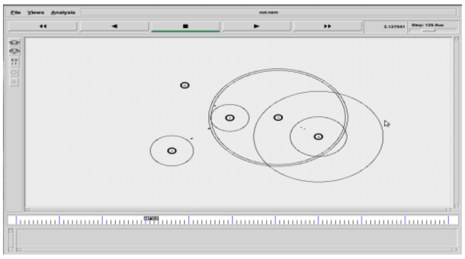


PDF Vs Time

Scanerio for Sinkhole Attack :



With attack

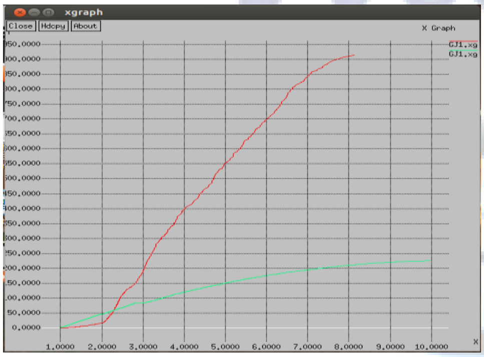


After attack removal

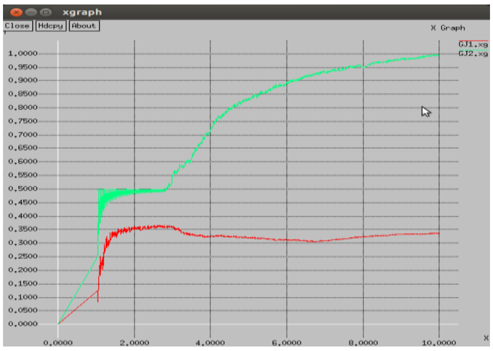
Performance Evaluation :

Red line shows with malicious node and Green line depicts the absence of malicious node.

1. **Delay :** It is the average time taken by data packets to reach the destination is known as delay or delay time.
2. **Packet Delivery Fraction :** Ratio of the number of packets received at destination to the number of packets sent from source.



Delay Vs Time



PDF Vs Time

Conclusion and Future Scope

This chapter concludes the whole research work done during the periods of time and the future work that can be done on basis of this study. Based on the general observations of the simulation results and support of literature review the following conclusion is made.

Security is an important issue in Wireless Sensor Networks. Malicious nodes may cause serious harmful to the security. The objectives listed have been achieved. In the presented work, we have discussed all the modes of AODV (Simple Mode, During Attack and Removal of Attack) along with their working. We hope that our work will contribute in providing further research directions in the area of security.

In our study we analyzed that flooding and sinkhole attack with respect to the performance parameters Delay and Packet Delivery Fraction. In a network it is important for a protocol to be efficient in term of security. We have analyzed the vulnerability of AODV protocols have more severe effect when there is higher number of nodes and more route requests.

With the results of AWK programming and Xgraph, we can show that in the case of simple AODV there is no packet drop and throughput is approximate 100%. But when attack occurs in the network, throughput decreases.

As the malicious node enters into the network, it drops the packets in the path. The performance of the network degrades. During attack Packet Delivery Fraction and throughput decreases and delay increases. But after removal of attack, Packet Delivery Fraction and throughput increases and delay in delivery of packets decreases.

Future scope is to devise new techniques for prevention of attack on various layers of the wireless sensor network layered framework which have been discussed earlier.

References

[1] Haowen Chan and Adrian Perrig, “Security and Privacy in Sensor Networks”, IEEE, October 2003, pp. 103-105.

[2] Curiac, D.-I., Plastoi, M., Banias, O., Volosencu, C., Tudoroiu, R., Doboli, A.: “Combined malicious node discovery and self-destruction technique for wireless sensor networks”. Int. Conf. on Sensor Technologies and Applications, 2009, pp. 436–441

[3] Lazos, L., Hirloc, P.R.: “High-resolution robust localization for wireless sensor networks”, IEEE J. Sel. Areas Commun., 2006, 24, (2), pp. 233–246

[4] Anjum, F., Pandey, S., Agrawal, P.: “Secure localization in sensor networks using transmission range variation”. IEEE Int. Mobile Ad Hoc and Sensor Systems Conf., November 2005, vol. 9

[5] Anthony D. Wood, John A. Stankovic, “Denial of Sevice in Sensor Network”, IEEE 2002.

[6] S.H.Jokhio, I.A.Jokhio, A.H.Kemp, “Node capture attack detection and defence in wireless sensor networks”, IET 2011.

[7] http://www.dees.unict.it/users/bando/files/wsn.pdf

[8] http://www.ijareeie.com

[9] http://ict4dconsortium.rhul.ac.uk/elgg/action/file/download?file_guid=7764

[10] http://nile.wpi.edu/NS/

[11] Z.A.Baig, “Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks”, Elsevier 2010, pp. 468-484.

[12] ZHANG Yi-ying, LI Xiang-zhen, LIU Yuan-an, “The detection and defence of DoS attack for wireless sensor network”, Elsevier 2012, pp. 52-56.

[13] Ana Paula, Marcelo H.T. Martins, Bruno.P.S.Rocha, “Decentralized Intrusion Detection in Wireless Sensor Networks”, ACM 2005.

[14] Nabil Ali, S.Khan, Bilal Shams, “Intrusion Detection Systems in Wireless Sensor Networks: A Review”, Hindawi Publications, 2013.

[15] Sahabul Alam, Debashis De, “Analysis of security threats in Wireless Sensor Network”, IJWMN, 2014.