ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 6, June 2017

Intruder Detection In Wireless Sensor Networks Using Crsa Algorithm

[1] Gowtham kumar Kavuturu, [2]Nelanuthala Karthik, [3]Ajit Kumar, [4]Avinash Kumar Tripathy,
[5]Mrs. J. Ahalya Mary (M.E)
[1] [2] [3] [4]B.Tech, Department of CSE SRM University, Ramapuram Campus Chennai, India
[5]Asst. Prof, Department of CSE SRM University, Ramapuram Campus Chennai, India
[1]gowthamkavuturu@gmail.com

Abstract: ***In the unstable wireless channel in Wireless Sensor Networks (WSNs), the packet loss rate may vary from time to time. It may also be very high in certain networks in the different time slots. The main problem when the packets are dropped at a sensor node is that it is very difficult to distinguish between the normal packet drop and the malicious packet drop. So, we propose a Reputation System which is aware of the channel with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. The algorithm will process the behavior of sensor nodes during the forwarding attacks according to the deviation between monitored packet loss and the estimated normal loss. To optimize the detection accuracy of CRS-A, we find the optimal threshold for forwarding detection, which is adaptive to the time- varying channel condition and the estimated packet loss probabilities of compromised nodes.. The selective forwarding attacks are often hindered by the normal packet losses, complicating the attack detection. Therefore, it is difficult to detect the selective forwarding attacks and improve the overall network performance. Most of related work focus on monitoring the packet losses in each transmission link and separating the nodes with higher packet loss rates from the data forwarding path. The other solutions are not effective in detecting selective forwarding attacks as that of the proposed technique since the main difficulty of attack detection is to distinguish the malicious drop from normal packet loss. The normal packet loss rate in the transmission link that is used should be considered in the forwarding evaluation.***

Key Words: Wireless Sensor Network (WSN), Reputation System, Channel-Aware, Packet Drop, Malicious Node, Malicious Drop

I. INTRODUCTION

Wireless sensor network (WSN) has been applied widely to both military and civilian applications as a promising event monitoring and data gathering technique. The WSNs are deployed in areas where they cannot be attended manually and even hostile environments to perform mission-critical tasks which include battlefield reconnaissance and internal security monitoring. However, due to the lack of physical protection, sensor nodes are easily vulnerable to adversaries, making the WSN vulnerable to various security threats in the real time scenario. Wireless sensor networks (WSNs) are vulnerable to different types of security threats which can ultimately degrade the performance of the whole network; that might result in fatal problems in a sensor network like denial of service (DoS) attacks, routing attacks etc. Key management protocols, authentication protocols and secure routing are not effective in providing security to WSNs for these types of attacks. Intrusion detection system (IDS) is a key solution to this problem. It analyzes the network by collecting sufficient amount of data and detects abnormal or the unusual behavior of sensor node(s). IDS based security mechanisms proposed for other network paradigms such as ad hoc networks, cannot be directly used in WSNs for the detection purpose. Researchers have proposed various intrusion detection systems for wireless sensor networks during the recent years making the sensor networks more effective. Wireless sensor networks (WSNs) are typically distributed, infrastructure-less, scalable and dynamic in nature. WSNs are vulnerable to several types of security threats that can degrade the overall performance of these sensor networks. Key management, authentication protocols and secure routing protocols cannot be effective for this particular purpose. In other words, these mechanisms can protect the network from outside attacks but fails against inside attacks in a sensor network.. In an outside attack, when an intruder tries to get access to the data in a network, it can be detected using several methods. In an inside attack, sensor node that is a part of the sensor network starts performing maliciously and gets access to the received data packets in the network.

II. PROPOSED SYSTEM

In the proposed system, the Channel Aware Reputation System Algorithm (CRSA) is used to determine the node as either normal node or the attacker node. The node designated as the malicious node is dropped from usage in the network. The

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 6, June 2017

existing systems drop the node even if they are not malicious and this problem is solved in the proposed system as the new system drops only the malicious nodes but not all the nodes that are dropping the data packets.

III. CRSA ALGORITHM

The CRSA Algorithm contains a threshold value. The threshold value is the minimum number of data packets that have to be transmitted in order for a node to be normal node and not the attacker node. The threshold value is determined by considering various factors that are responsible for the packet loss in a Wireless Sensor Network. The different causes for the packet loss in a WSN are the MAC layer collisions and the channel related problems.

i)MAC Layer Collisions: This type of loss occur due the collision or the overlapping of the MAC layers of the different devices. These collisions result in the loss of the data packets and thereby deteriorating the overall performance of the channel and the performance of the network.

a) Node Creation and Configuration: Node creation is nothing but the creation of the wireless nodes in the network scenario that is decided. Node ii)Channel Related Problems: The different channel related problems like the noise, disturbances in the air, performance and limitations of the different devices cause the certain data packets to be dropped at the various nodes.

The threshold value or the minimum value is fixed taking into account all the natural and unavoidable causes in the current network. The node(s) which is having the packet loss less than that of the value prescribed is taken as the normal node and that particular packet drop is the normal drop. The node(s) having the packet loss more than the value at them is called the malicious or the attacker node and that packet drop is called the malicious drop. The proposed concept can be executed in a six step process which ultimately simulates the proposed concept.

They are

a) Node creation and configuration.
b) Forwarding node selection
c) Normal Packet loss Estimation
d) Reputation system
e) Malicious Node Identification

Performance Evaluation

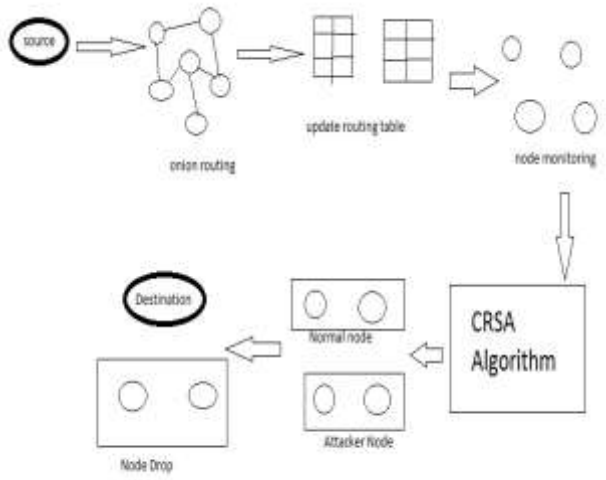

Figure 1:Architecture Diagram

configuration essentially consists of defining the different node characteristics before creating them. They may consist of the type of addressing structure used in the simulation, defining the network components for mobile nodes, turning on or off the trace options at Agent/Router/MAC levels, selecting the type of ad-hoc routing protocol for wireless nodes or defining their

energy model. Simulator::node-config accommodates flexible and modular construction of different node definitions within the same base Node class. For instance, to create a mobile node capable of wireless communication, one no longer needs a specialized node creation command.

b)*Forwarding Node Selection:* The forwarding node is selected based on the source and destination. The next node is selected iteratively from the previous node. The distance between the nodes plays a crucial role in selecting the next node to be used. The node having the shortest path is selected for handing over the data packets. In other words, it uses the Open Shortest Path First (OSPF) algorithm to select the nodes between the source and destination.

c) *Normal Packet Loss Estimation:* The normal packet loss should be considered into the forwarding behavior evaluation for sensor nodes. According to the network model, normal packet loss is mainly caused by the poor and unstable wireless channel and MAC layer collisions. The poor and unstable radio link quality is the primary reason for the time-varied packet losses. The estimated normal packet loss is very crucial for the proposed system as it will be used to determine whether a particular node is malicious or not.

d) *Reputation System:* The Reputation System consists of the two components namely Reputation Evaluation and Reputation Propagation.
Reputation Evaluation: The each node is evaluated individually for the packet loss at that particular node in the given time. Each node is given its own reputation value based on the individual packet loss at the given particular node.
Reputation Propagation: In the reputation propagation, the reputation value is propagated within the given network so that the other nodes can know the packet loss at a particular node.

e) *Malicious Node Identification*: In each Tt, sensor nodes can evaluate the forwarding behaviors of their next hop sensor nodes and update their reputation table with the above procedures. After a number of evaluation periods, the reputation values of malicious nodes are significantly reduced in the reputation tables of their neighboring nodes.

f) *Performance Evaluation:* During simulation time the events are traced by using the trace files. The performance of the network is evaluated by executing the trace files. The events are recorded into trace files while executing record procedure. In this procedure, the events like packet received, Packets lost, Last packet received time etc are traced. These trace values are write into the trace files. This procedure is recursively called for every 0.05 ms. so, trace values recorded for every 0.05 ms.

IV. REAL TIME APPLICATION

The proposed system can be very useful in the real time applications where the identification of attacker node is very important. The proposed system does not take care about the packets already lost and thus it can be used in area where preventing the future loss of packets is very important than the packets that are already lost during the transmission.

V.CONCLUSION

The concept was proposed to find the attacker or the compromised node within the network. There are several other techniques to find the outside attacker node but it is difficult to find if a node within sensor network is compromised. It is also important to differentiate the normal packet drop and the malicious packet drop.

VI Future Work

The proposed system can be improved by the further research. As the system ignores the packets that are lost at the malicious node(including normal nodes), a way can be developed to retransmit the data packets that are lost at the nodes.

Furthermore, different algorithms can be used to select the forwarding node or the next node. The algorithm used may be affected by different parameters like the type of network used, characteristics of the nodes, topology, purpose of the network etc,.

The system can be made even more efficient by employing the different new methods to determine the threshold value as the nodes with the packet loss value more than that of threshold value is considered as the malicious node in the proposed system.

VII.References

1) “Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks” by Ju Ren,Yaoxue Zhang, Kuan Zhang, Xuemin Shen.

2) Intrusion Detection Systems for Wireless Sensor Networks by Ashfaq Hussain Farooqi and Farrukh Aslam Khan.

3) Functional reputation based reliable data aggregation and transmission for wireless sensor networks by Suat Ozdemir.

4) A repeated game approach for analyzing the collusion on selective forwarding in multihop wireless networks by Dong Hao , Xiaojuan Liao , Avishek Adhikari , Kouichi Sakurai , Makoto Yokoo.

5) AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks by Yu Zhang, Loukas Lazos, William Jr. Kozma