International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Identification of Denial-of-Service Attacks in Wireless Sensor Networks

E. Gayathiri[1]
[1]Department of CSE, P.A College of Engineering and Technology, Coimbatore, TamilNadu

Abstract **- In Wireless Sensor Network (WSN), security is one of the most challenging issues. An attacker can launch different attacks to disrupt the communications by dropping packets in WSN. Packet dropping comes under the category of Denial-Of-Service attacks. Many methods have been proposed to catch such attacks. The proposed method is effective, which can efficiently and effectively detect the misbehaving forwarders. Detailed analysis and simulation have been performed to find the effectiveness and efficiency of the proposed scheme using ns2 simulator.**

Index terms **- Intruder, packet dropping, sink, sensor node, wireless sensor networks.**

I. INTRODUCTION

Wireless Sensor Networks (WSN) is a new class of emerging networking technology consists of tiny, sensor devices, called sensor nodes. Sensor node is a collection of memory, processor, hardware and battery. Sensor networks mainly use broadcast communication. Sensor nodes may not have global id because of the large amount of overhead and large amount of sensors. Sensor devices are used to monitor the physical environment.WSN is built of several hundred or even thousands of small sensor nodes.WSN are self-healing and self-organizing networks. Nodes in self-healing networks have the capability to reconfigure their link associations and find alternative pathways around compromised node, failed or powered-down nodes. In self organizing networks new nodes can easily join to existing sensor networks. Sensor networks are used as key for the creation of smart spaces, both in home and work environments.

WSN consists of gateway or base station which can communicate with number of sensor nodes. The gateway can be connected to end user through internet as shown in Figure1. Sensor nodes are used to monitor both area and object. This new technology is used in various fields to monitor the environment. Numerous application areas includes health monitoring, indoor climate control, area monitoring, military monitoring, acoustic detection, entertainment and inventory.

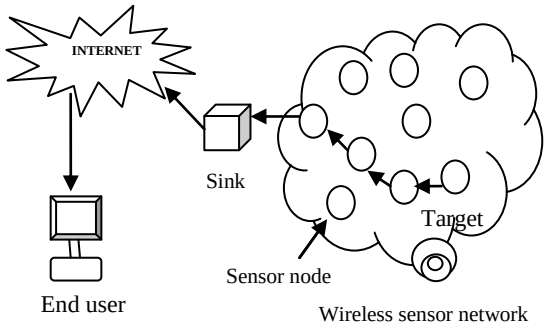

Figure1: Wireless Sensor Network.

Most of the wireless sensor devices are expected to work in a possibly adverse or even unattended environment. It is easy for an adversary to physically pick up and compromise sensor nodes in hostile environment. An attacker can launch various attacks [1] after compromising sensor nodes to disrupt the multi-hop wireless communication. An important attack among various types of attacks is *packet dropping*, i.e., instead to forward packets, compromised nodes drop the packets. Packet dropping attack comes under Denial of Service attacks.

A. Need for Security in Sensor Networks

Security is a great challenge in wireless sensor networks due to various reasons. Placement of sensor nodes in non-monitoring and unreachable environments makes sensors nodes vulnerable to security compromise and lead to physical capture. Sensor nodes are resource constrained in terms of battery, memory, CPU, communication bandwidth and using radio link communication.

The implementation of WSN with high security and privacy must simultaneously address several difficult research challenges. The wireless communication increases the vulnerability of the network to eavesdropping, packet modification, packet dropping, unauthorized access, spoofing, replay and denial-of-service (DOS) attacks among sensor nodes. The resource constraints in sensor nodes limit the

IJERT

implementation of encryption, decryption and authentication on individual sensor nodes.

WSN face the physical security risk of individual sensor nodes falling into the unauthorized hands. Sensor nodes that are deployed in the field can be obtained by an intruder and can then be subject to attacks by potentially well-equipped intruder in order to compromise a single resource node. Following a successful attack, a compromised sensor node could then be used to instigate malicious activities, such as advertising false routing information and launching DOS attacks within the sensor network. Intruder mostly chooses shortest path to compromise the sensor node.

B. Attack Models in Wireless Sensor Network

1) *Sinkhole attacks:* This attack makes the compromised node attractive to other sensor nodes based on routing choice.
2) *HELLO flood attacks:* Nodes broadcast HELLO packets and increases the traffic.
3) *Selective forwarding:* Nodes selectively drops few packets instead of forwarding.
4) *Sybil attacks:* A single node creates multiple identities to other nodes in the network.
5) *Wormholes:* Adversary receives the message in one part and replays the message in different parts**.**
6) *DOS Attacks:* Packet modification and dropping are types of DOS attacks which modify or drop the packets.

.

II. RELATED WORKS

Existing solutions for detecting packet dropping in wireless sensor networks are monitoring individual nodes and multipath routing [2], [3], [4], [5], is an alternative routing technique to single path routing, which selects multiple paths to deliver data from source to destination. Multipath routing uses redundant paths to transmit the data. Multipath routing can largely address the reliability, [6], [7], [8], security and load balancing issues of single path routing protocols.

To identify packet droppers, it has been proposed that probing technique is used to detect the malicious packet dropping attack. In this approach, every node proactively monitors the forwarding behaviors [9], [10], of their neighbors to determine if the neighbors are compromised node. A resilient packet-forwarding scheme uses Neighbor Watch System (NWS) against maliciously Packet-dropping nodes in sensor networks. This method involves high energy cost.

The proposed method uses node categorization algorithm. In this effective scheme Direct Acyclic Graph (DAG) is established at the sink. When data are transmitted from source to sink, each packet sender and intermediate nodes adds some extra bits to the packet called packet marks. The information in the packet marks is very useful for sink to run node categorization algorithm. The sink can calculate the dropping ratio for every sensor node in WSN. The dropping ratio can be calculated based on number of packets received to the total number of packets sent. The sink runs proposed node categorization algorithm to catch nodes that are droppers.Node categorization algorithm categorizes sensor nodes into good nodes and bad nodes

Compared with existing schemes, proposed scheme has the following unique characteristics: (1) effective in identifying packet droppers, (2) detection rate of malicious node is high. Extensive simulation on ns2 simulator has been conducted to verify the effectiveness and efficiency of the proposed scheme in various scenarios.

The rest of the paper is organized as: Section II defines related work, Section III describes the system model and section IV reports the performance evaluation. Section V reports the conclusion of the paper.

III. SYSYEM MODEL

A. Assumptions

In WSN a large number of sensor nodes are distributed to monitor the physical conditions of hostile environment. Sensor nodes are responsible for collecting sensory data and forwards packet, containing information towards a trustworthy sink. After distribution, all sensor nodes send information about their neighboring autonomous sensor nodes to the sink. Hence sink is aware of wireless network topology.

B. Attack Model

Packet *dropping:* Packet dropping attack also called black hole attack, in which an autonomous sensor node that is supposed to relay packets instead drops them. This happens when sensor node is compromised by an attacker. Packet dropping happens under following reasons, which can be grouped into different categories,

1) Due to transmission medium: Due to contention, a packet may be dropped in physical medium. A packet may be dropped due to traffic or corruption in the physical medium.
2) Lack of energy: Due to Buffer overflow, a packet may be dropped. A packet can also be dropped due to shortage of energy resources.
3) Due to compromised node: A packet may be dropped due to malicious act of an attacker node.

There is an assumption that adversary cannot compromise regular sensor nodes during DAG establishment and the sink is trustworthy and cannot be compromised by intruder.

C. Detection of misbehaving forwarders

The proposed scheme consists of various phases such as node deployment phase and intruder identification phase. In the node deployment phase, network topology is formed by sensor nodes, called DAG. A routing tree is formed from the

IJERT

DAG. Data will be reported to the sink follow the routing tree structure.

In each round, each source node and an intermediate node transmits the packet by adding some additional bits to the packet. Each sensor node encrypts the packet with shared unique symmetric key. Sink runs the proposed node categorization algorithm by using additional information in the received packets. The node categorization algorithm is used to detect the malicious nodes (i.e., packet droppers).

The routing topologies is reshaped every round, the sink will have collected information about malicious node in different routing topologies.

1) Tree establishment and Packet transmission: Sensor nodes in the network form a tree structure called DAG. The sink knows the routing topology and share the symmetric key with each sensor node. When a sensor node sends out a packet, it adds the sequence number to the packet. Each sender or forwarder encrypts the packet with unique key shared with the sink. When an intermediate node receives a packet, it adds some extra bits to the packet to mark the routing path of the packet, encrypts the packet and transmits to its parent node.

When an intermediate node is compromised by an attacker it may drop the packets it receives. After receiving a packet, the sink decrypts the packet to get the information about the original sender and packet sequence number. Sink calculates the dropping ratio for every sensor node by tracking the sequence number of the packet for every time interval called round. With the help of network topology and dropping ratio sink identifies the malicious node.

2) Key sharing: The purpose of key sharing is to exchange secret symmetric keys between the sink and every regular sensor nodes. It involves establishment of routing tree and DAG to allow packet transmission from every sensor node to the sink.

Keys and other system parameters are preloaded in each sensor node u.

Ku: a secret symmetric key shared between every sensor node and sink.

Lr: represents duration of round. Sink checks the sequence number of received packets, for each certain time period called round.

Np: represents number of parent nodes in routing tree for every sensor node to reach sink.

Ns: represents packet series number or sequence number. The first packet sequence number of every sensor node is 0 and so on.

3) Packet Transmission: Every sensor node counts the number of packets sent so far with the help of counter cp. when a node wants to send data to the sink, it transmits the packets to its parent node. When a sink receives packets, it runs node categorization algorithm to categorize nodes as bad nodes and good nodes.

4) Node Categorization Algorithm: Sink runs node categorization algorithm for every sensor node. In every round, for each sensor node *u*, the sink node *s* keeps track of the number of packets sent from *u* and the number of packets received to *s*. In the end of each round, the sink node *s* calculates the dropping ratio based on number of packets sent and number of packets received for each node *u*. *Nt is* the number of transmitted packets and *Nr* is the number of received packets. The dropping ratio (*dr*) for every sensor node is calculated as

$$dr = \frac{((Nt - Nr) * Nt)}{(Nt + Nr) + (Nt * (Nt - Nr))}$$

Based on the dropping ratio value of every sensor node and the tree topology, the sink identifies malicious node for sure and may be malicious node. Due to energy loss or congestion, the nodes may drop the packets. If transmitted packets are not intentionally dropped by forwarding nodes, then dropping ratio of this node should be less than θ. The value of θ should be greater than 0. Assume the value of θ value is 0.5. The nodes can be categorized into three cases (i) packet droppers for sure. (ii) Suspicious packet droppers. (iii) No packet droppers for sure. Sink runs node categorization algorithm for every sensor node in T and the following cases exist.

Case 1: If the dropping ratio is less than θ, then a node is called good node (not dropped packets) or the node is called as suspiciously bad (suspected to have dropped packets).

***Case 1.1*:** If the dropping ratio value is equal to zero, then the node has not dropped packets.

***Case 1.2*:** If the dropping ratio is greater than zero but less than θ, then the node is called suspiciously bad node.

***Case 2*:** If the dropping ratio is greater than θ, then a node is called bad for sure (must have dropped packets).

The dropping packets may due to traffic, collisions, and malicious node. Based on the above result, a node categorization algorithm is used to find nodes that whether the node is bad node, suspiciously bad, or good node. Tree used to forward data is dynamically changed for every time interval and each sensor node may have a different parent node which is called tree reshaping.

Algorithm1: Node Categorization Algorithm

1. Input Tree T, with each node u, dropping ratio dr,
   threshold value Θ, Sink node s
2. for every sink node in T do
3. find dropping ratio du
4. if dr < Θ then
5. Set u as good for sure or suspiciously bad;
6. if dr = 0 then
7. Set u as good for sure

IJERT

8. else if dr > 0
9. set u as suspiciously bad
10. else
11. break;
12. else
13. set u as bad for sure
14. repeat

The value of Θ can be taken as 0.5.Packets may also be dropped due to loss of energy or due to traffic.

IV PERFORMANCE EVALUATION

The performance of the proposed scheme is evaluated by using ns-2 simulator. Two metrics are used to measure the performance of the proposed scheme: detection rate, defined as the ratio of identification of malicious nodes successfully and packet delivery rate, defined as the ratio of number of packets received to the number of packets sent to the sink.

A. Simulation Model and Parameters

Simulations runs on a 1000m x 1000m network with randomly generated network topology. Packet size is 512 bytes. The size of the network is 20 nodes and the percentage of bad nodes is set as 2%.Packet reporting interval per node is 3 seconds and the length of each round is 200 seconds. When compromised node wants to drop packets it drops 30% of total packets.

B. Simulation Results

Simulation results have been reported by comparing node categorization algorithm with probing technique and multipath forwarding methods. The deployment of sensor nodes in tree structure and dropping of packets by malicious nodes is shown in figure 2. Sink node shares symmetric key with every sensor node for encryption and decryption of packets. With the help of secret key sink node decrypts the packet and find useful information to run node categorization algorithm.

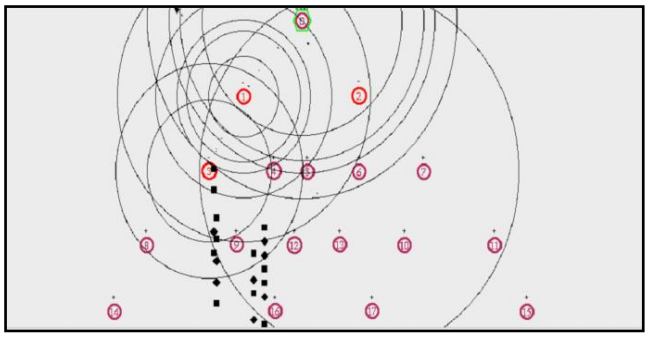

Figure 2: Deployment of sensor nodes

Figure 3 shows the categorization of good nodes and bad nodes of the proposed scheme. Node categorization algorithm categorizes sensor nodes as good nodes and bad nodes. "+" symbol indicates good nodes and "-" symbol indicates bad nodes. Each node connects to its parent node.

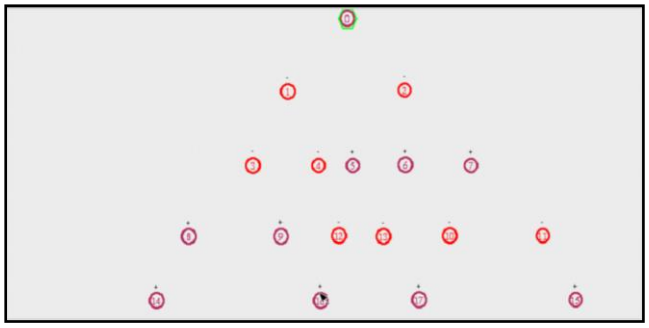

Figure 3: Categorization of good nodes and bad nodes

Figure 4 shows the detection rate of misbehaving nodes of the proposed scheme and the impact of the threshold. From the figure existing methods like multipath routing and probing technique provides lower detection rate when compared to node categorization algorithm.

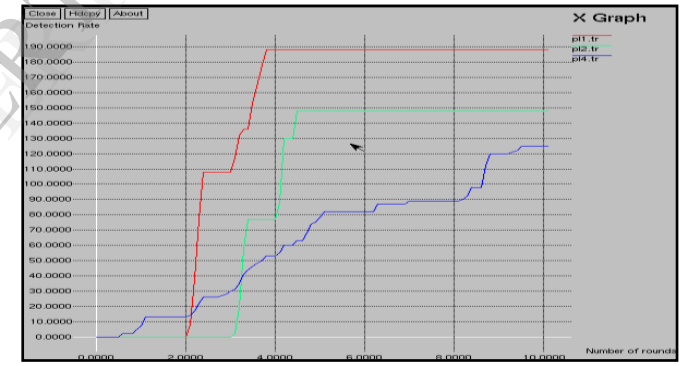

Figure 4: Detection rate of misbehaving nodes

V. CONCLUSION

The proposed method is simple and effective scheme in identifying packet droppers that will disrupt the communication in WSN. The sink calculates the dropping ratio of every sensor node. Sensor node behaviors can be analyzed by changing the tree structure for every round. Most of the malicious nodes are identified by node categorization algorithm. Detailed analysis and simulation have been conducted to verify the effectiveness of the scheme

IJERT

REFERENCES

[1] H.Chan and A. Perrig, "Security and Privacy in Sensor Networks," *IEEE Computer*, October 2003.

[2] Karlof and D. Wagner, "Secure routing in wireless sensor networks:attacks and countermeasures," *the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, May 2003.

[3] V. Bhuse, A. Gupta, and L. Lilien, "Dpdsn: Detection of packet-dropping attacks for wireless sensor networks," *In the Trusted Internet Workshop,International Conference on High Performance Computing*, December 2005.

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *ACM MobiCom*, August 2000.

[5] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," *Third IEEE Annual Consumer Communications and Networking Conference (CCNC)*, pp. 640–644, Jan. 2006.

[6] S. Lee and Y. Choi, "A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks," *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks (SASN)*, pp. 59–70, 2006.

[7] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-route Filtering of Injected False Data in Sensor Networks," *IEEE INFOCOM*, March 2004.

[8] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data in Sensor Networks,"*IEEE Symposium on Security and Privacy*, 2004

[9] F. Ye, H. Yang, and Z. Liu, "Catching Moles in Sensor Networks," *IEEE International Conference on Distributed Computing Systems (ICDCS)*, June 2007.

[10] Q. Li and D. Rus, "Global clock synchronization in sensor networks,"*IEEE INFOCOM*, 2004.

[11] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc*), May 2005.

[12] Z. Yu and Y. Guan, "A Dynamic En-route Scheme for Filtering False Data in Wireless Sensor Networks," *IEEE Infocom 2006*, April 2006.

IJERT