ISSN: 2320-1363

An Effective Filtering of Packet Dropping and Modification in WSN

Mahabub Subhani.Sk*1, P Ramesh Babu*2

M.Tech (CSE) Student Department of CSE, Priyadarshini Institute of Technology & Science, Chintalapudi, Guntur(Dist), Ap, India.

Associate Professor, Department of CSE in Priyadarshini Institute of Technology & Science, Chintalapudi, Guntur(Dist), Ap, India

Abstract

In Wireless Sensor Network, sensors at different locations can generate streaming or discrete data, which can be analyzed in real time or non real time to identify events of interest. A sensor node is often placed in an unfriendly environment, to perform the monitoring and data collection tasks. When it is unfriendly environment, node may subject to compromise. In this paper two algorithms are proposed firstly, one node categorization algorithm to identify nodes that are droppers or modifiers for sure or suspicious droppers or modifiers. The packet droppers and modifiers are common attacks in wireless sensor networks. It is very difficult to identify such attacks and this attack interrupts the communication in wireless multi-hop sensor networks. We can identify the packet dropper and packet modifiers using ranking algorithms and packet marks. The performance is represented using detection rate and false positive probability. The proposed scheme provides an effective mechanism for catching compromised node.

Keywords: Packet Droppers And Modifiers, Intrusion Detection, Wireless Sensor Networks.

1. Introduction

In wireless sensor networks consists of large number of small sensor nodes having limited computation capacity, restricted memory space, limited power resources, and shortage radio communication device. With a widespread deployment of these devices, one can precisely monitor the environment. Basically, sensor network are application dependent and sensor nodes monitor the environment, detect events of interest, produce data, and collaborate in forwarding the data toward a sink, which could be a gateway, base station, storage node, or querying user. Securing the wireless sensor networks need to make the network support all security properties: confidentially, integrity, authenticity and availability. A sensor network often deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward.

We expect sensor networks to consist of hundreds or thousands of sensor nodes as in Fig 1.1 Each node to represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who capture and reprogram individual sensor nodes. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the adversary can then mount a variety of attacks.

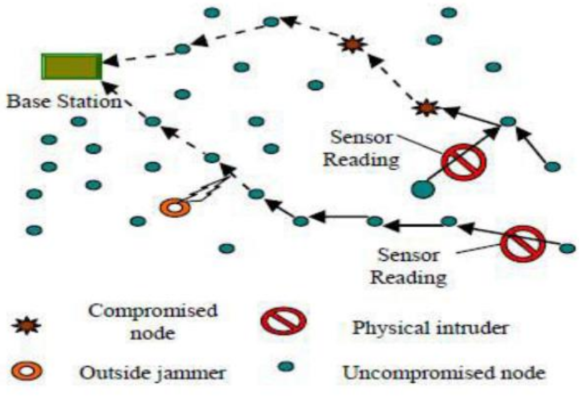

Fig1.1. Sensor Network

Packet dropping is nothing but a bad node drops all or some of the packets that are supposed to be forwarded. It may also drop the data generated by itself for some malicious purpose such as blaming innocent nodes. This paper proposes a scheme to catch both packet droppers and modifiers. At first routing tree is established using DAG. Data is transmitted along the tree structure toward the sink. A packet sender or forwarded adds a small number of extra bits, which is called packet marks, is designed such that sink can be obtain the dropping ratio associated with every sensor node. Node categorization algorithm to identify nodes that are droppers or modifiers for sure or are suspicious dropper/modifiers.

2. Related Work

There are three types of existing approaches to detect packet dropping attacks. They are multipath forwarding approach, neighbor monitoring approach, and acknowledgement approach. Multipath forwarding is a widely adopted countermeasure to mitigate packet droppers, which is based on delivering redundant packets along multiple paths. Another approach is to exploit the monitoring mechanism. The cache array routing protocol is the most notable hash based cooperative caching protocol. The rationale behind CARP constitutes load distribution by hash routing among web proxy cache arrays. A mobile doesn’t know whether the data source or some other nodes serve its request. If multiple data sources exist, or if the mobile node doesn’t know where the data source is, Hybrid Cache might not be a good option. In addition catching nodes outside the path between the requesting node and the data source might not ne able to share cache information with the requesting node.

3. Proposed system

We simulate our caching algorithm in different ad-hoc network scenarios and compare them with other caching schemes, showing that our solution succeeds in creating the desired content diversity, thus leading to a resources efficient information access. The sink can figure out the dropping ratio associated with every sensor node, and then runs our proposed node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. Specifically, based on the packet marks, the sink can figure out the dropping ratio associated with every sensor node, and then runs our proposed node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. Data caching strategy for ad hoc networks whose nodes exchange information items in a peer to peer fashions. These decisions are made depending on the perceived "presence" of the content in the nodes proximity, whose estimation does not cause any additional overhead to the information sharing system. However the solution that was proposed is based on the formation of an overlay network composed of mediator nodes and it is only fitted to static connected networks with stable links among nodes. We proposed to mitigate or tolerate such attacks, but very few can effectively and efficiently identify the intruders. To address this problem, we propose a simple yet effective scheme. This can identify misbehaving forwarders that drop or modify packets. Extensive analysis and simulations have been conducted to verify the effectiveness and efficiency of the scheme.

3.1 list of modules:

I. Node Configuration
II. Sender Node
III. Intermediate Node
IV. Sink
V. Verify
VI. Merge Packets
VII. Categorization And Ranking

Module Description

Node Configuration

a) Link Configuration

In this module nodes are configured based on number of nodes in group. We create the network group by connecting nodes to sink. Link configuration means connecting the nodes and intermediate nodes to the sink. In every round, for each sensor node u, the sink keeps track of the number of packets sent from u, the sequence numbers of these packets, and the number of flips in the sequence numbers of these packets, (i.e., the sequence number changes from a large number such as N_s - 1 to a small number such as 0). In the end of each round, the sink calculates the dropping ratio for each node u. Suppose $n_{u,max}$ is the most recently seen sequence number, $n_{u,flip}$ is the number of sequence number flips, and $n_{u,rcv}$ is the number of received packets.

ISSN: 2320-1363

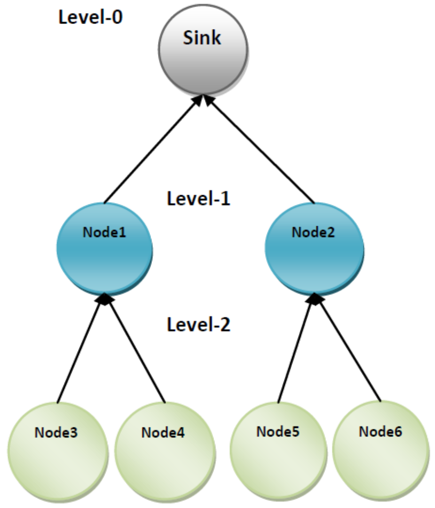

Fig3.1.1 structure of node configuration

Sender Node

a) Packet Splitting

In this module, sender selects the file which is to be sent. And then it split into the number of packets based on the size for adding some bits in it.

b) Send Packets to Intermediate

And then it encrypts all the splitted packets. And then sender adds some bits to each encrypted packets before sending that. Bit addition for each packet is identification for sender. After adding of bits to each packet, it sends the packets to the nearest node or intermediate node.

Intermediate Node

a) Send Packets to Sink

In this module, the intermediate node receives packets from the sender. After receiving all packets from sender, it encrypts all packets again for authentication. Before sending to sink intermediate add some bits to each packet for node identification. After adding some bits from intermediate, is sends all packets to the sink.

b) Modify or Drop

Before sending all packets to sink, packets dropping or packets modifying may be occur in intermediate.

Sink

a) Verify

In this module, sink receives all packets from the sender node, and it verifies all packets from the sender node, and it verifies all packets which are dropped or not. and it also verifies the packets which are modified or not and it can identify the modifiers in the process based on the bit identification.

b) Merge packets

After receiving all packets in sink, it decrypts all packets. After the decryption if there is no modified or dropped packets, it merge all packets. After merging, sink can receive the original file.

c) Categorization and ranking

In this module categorization and ranking will be performs based on the node behavior. If there is any modification or drop of packets in node it assumes negative value for modifier or dropper. Sink performs ranking for each node based on the category of nodes. Sink gives ranking like Good, Temporarily Good, suspiciously Bad, Bad based on the node behavior in the process.

4. CONCLUSION

We propose a simple yet effective scheme to identify misbehaving forwarders that drop or modify packets. Each packet is encrypted and padded so as to hide the source of the packet. The packet mark, a small number of extra bits, is added in each packet such that the sink can recover the source of the packet and then figure out the dropping ratio associated with every sensor node. The routing tree structure dynamically changes in each round so that behaviors of sensor nodes can be observed in a large variety of scenarios. Finally, most of the bad nodes can be identified by our heuristic ranking algorithms with small false positive.

REFERENCES

[1] H. Chan and A. Perrig, “Security and Privacy in Sensor Networks,” Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[2] V. Bhuse, A. Gupta, and L. Lilien, “DPDSN: Detection of Packet-Dropping Attacks for Wireless Sensor Networks,” Proc. Fourth Trusted Internet Workshop, 2005.

[3] M. Kefayati H.R. Rabiee, S.G. Miremadi, and A. Khonsari, “Misbehavior Resilient Multi-Path Data Transmission in Mobile Ad-Hoc Networks,” Proc. Fourth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN ’06), 2006.

[4] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, “Secmr—A Secure Multipath Routing Protocol for Ad Hoc Networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007.

[5] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical En-Route Filtering of Injected False Data in Sensor Networks,” Proc. IEEE INFOCOM, 2004.

[6] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An Interleaved Hop-by- Hop Authentication Scheme for Filtering False Data in Sensor Networks,” Proc. IEEE Symp. Security and Privacy, 2004.

[7] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, “Toward Resilient Security in Wireless Sensor Networks,” Proc. Sixth ACM Int’l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc ’05), 2005.

[8] M. Just, E. Kranakis, and T. Wan, “Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks,” Proc. Int’l Conf. Ad-Hoc

ISSN: 2320-1363

Networks and Wireless (ADHOCNOW ’03), 2003.

[9] R. Roman, J. Zhou, and J. Lopez, “Applying Intrusion Detection Systems to Wireless Sensor Networks,” Proc. IEEE Third Consumer Comm. Networking Conf. (CCNC), 2006.

[10] S. Lee and Y. Choi, “A Resilient Packet-Forwarding Scheme Against Maliciously Packet-Dropping Nodes in Sensor Net- works,” Proc. Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN ’06), 2006.

[11] I. Khalil and S. Bagchi, “MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks,” Proc. Fourth Int’l Conf. Security and Privacy in Comm. Netowrks (SecureComm ’08), 2008.