Detecting Intruders and Packet Modifiers in Wireless Sensor Networks

1Mr.Selvaraj.Navaneethan, 2Dr.A.Kathirvel, 3 G.Bharathikannan, 4Mr.N.Rajaragupathi, 5Mr.L.Ayyappan

1,3Assistant Professors, 2Professor, 4,5Network Engineers
1,3,4,5 Sembodai Rukmani Varadharajan College of Engineering
2 Anand Institute of Higher Technology, Chennai

Abstract: **Multicast transmission can create a data loss and packet modifiers in wireless sensor networks. A routing tree routed at the sink is first established. When sensor data are transmitted along with the tree structure towards sink. At each packet sender add a small number of extra bits called packet marks. The packet marks deliberately designed such that sink obtain useful information. The sink can figure dropping associated with every sensor by node categorization algorithm (NDS) to identify nodes that are dropped modifiers. Tree structure is dynamically changes every time that depend upon interval and behavior of nodes. Node behavior is accumulated periodically. The proposed algorithm identifies most likely bad nodes from suspiciously bad nodes. Soundness of the proposal will be tested in prominent Network Simulator.**

Key Words: **Multicast, NDS, Nodes**

1. INTRODUCTION

User can send a data to destination and eliminating the packet trappers and modifiers in networks. The secure transmission is based on the following services.Includes.system initialization, Directed acyclic graph, tree reshaping, node categorization, global ranking algorithm.

i. System initialization

The purpose of system initialization is to set up secret pair wise keys between the sink and every regular sensor node. Preloading keys and other system parameters

ii. Directed acyclic graph

In DAG establishment each sensor node randomly chooses the parent node from the records. This module is used to send the data. First find the active peers in network. Among the active peers source will choose the destination node. Then source will find all possible paths to reach the destination. It also calculates the weight of all paths.

After analyzing the weight, the source will decide one path through which the packet will be send. If none of the possible paths found is less than threshold level, then it is the time to reset the threshold value else can't send the message.

iii. Tree reshaping

Sensor node changes their parent node at a particular interval. This is called round. Each node in the selected path will just check the IP address in the data and decide whether are the intended user to receive the data or pass the data to the next node. Also send an ACK to the source indicating that it receives the message sent by it.

iv. Node categorization method

It is executed in the base station at each round. After executing the algorithm the sink calculates the dropping ratio for each node. The route has cost either smaller than or equal to the shortest single-path cost between two nodes includes the set of single-path routes between these nodes. Note that there may be multiple routes with equal minimal cost.

v. Global ranking method

Global ranking algorithm executed in the base station. After certain round is finished, this algorithm executed. It gets the certain round result from the node categorization algorithm. Whenever a node receives the data packet it finds the source of the packet and sends an ACK message. The source gets the ACK from the nodes in the selected path confirming that the data is passing over the intended path. After getting the ACKs from all the nodes in the selected path, it will decide that the message is sent to receiver and shows a pictorial representation of the path.

2. ARCHITECTURE DIAGRAM

Architectural diagram of our proposed system as shown in the Fig. 1.

2.1 BASIC SCHEME

Our target is to find out both packet droppers and modifiers. In this scheme, a routing tree rooted at the sink is first established. When sensor data are transmitted along the tree structure toward the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks, to the packet.

The format of the small packet marks is deliberately designed such that the sink can obtain very useful information from the marks. 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. As the tree structure dynamically changes every time interval, behaviors of sensor nodes can be observed in a large variety of scenarios.

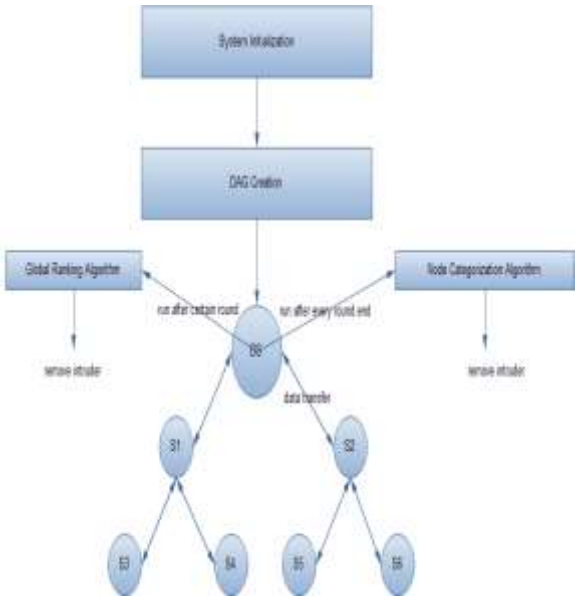

Fig. 1 Architecture Diagram

As the information of node behaviors has been accumulated, the sink periodically runs our proposed heuristic ranking algorithms to identify most likely bad nodes from suspiciously bad nodes. This way, most of the bad nodes can be gradually identified with small false positive.

Using this concept the data can be safely send to the destination. Once the packet modifiers and trappers are identified that particular node is eliminated from networks.

The duplication of data is eradicated so it consumes low energy levels.

2.2 NODE CATEGORIZATION

Here we propose a node categorization algorithm based on the nodes.

2.2.1 ALGORITHM

The node categorization consists of following steps:

1. Tree T, with each node u, and its Dropping Ratio

2. For every sink node in T do
3. Find all the dropping ration
4. if du<0 then
5, Set u as good or suspiciously node
6. If du=0 then
7. Set u as good node
8. else if du>0
9. Set u as bad
10. Else
11. Break;
12. set u as surely bad
13. Repeat

1. If the dropping rate is less than 0 then the node has not dropped any packets otherwise nodes may dropped a packets assume to be a suspiously node

2. If the dropping rate is equal to 0 then the node has not dropped any packets

3. If the dropping rate is greater than than 0 then the node has suspected to be dropping any packets

4. If the dropping rate is greater than than 0 then the node has suspected to be dropping any packets due to traffic, collisions and malicious node.

   Tree structure is dynamically changes in the regular interval of time

2.3 REQUIREMENTS TO THE SENDER

In our process the sender needs to add extra bit to each packet. Because it can provide a security level equivalent to conventional RSA and DSA with much shorter signature, the adding extra bit in operation is more efficient than the RSA signature generation. Moreover this technique can be implemented over elliptic curves. It is used to achieve secure transmission of data **at** the receiver.

2.4 ENHANCED SCHEME

The basic scheme targets at the packet loss problem, intruders and modifiers which is inherent in the internet and wireless networks. It has perfect resilience to packet loss no matter whether it is random loss or burst loss. In some circumstances, however, an attacker can inject forged packets into a batch of packets to disrupt the extra bits added to the each packet for verification, leading to Dos. A naive approach to defeat the Dos attack is to divide the batch into multiple smaller batches and perform batch verification over each smaller batch and this divide and conquer approach can be recursively carried out for each smaller batch which means contains extra bit for verifications at each receiver. In worst case the attacker can inject forged packets at very high frequency and expect that each receiver stops the batch operation and recovers the per packet signature verification which may not be viable at resource constrained receiver devices.

In this section we present an enhanced scheme called global method, which combines the basic scheme that packet filtering mechanism to tolerate packet injection in particular, the sender attaches each packet with a mark which is unique to the packet and cannot be spoofed. At each receiver, the multicast stream is classified into disjoint sets based on marks. Each set of packets comes from either the real sender or the attacker. The mark design ensures the packet from the real sender never falls into any set of packets from the attacker. Next each receiver only needs to perform Batch verify () over each set.

If the result is TRUE, the set of packets is authentic. If not, the set of packets is from the attacker, and the receiver simply drops them and doesn't need to divide the set into smaller subsets for further verification. Therefore, a strong resilience to Dos due to injected packets can be provided.

3. PERFORMANCE EVALUATION

We evaluate performance [1 – 2] in terms of resilience to packet loss, efficiency and Dos resilience.

3.1. Resilience to packet loss

We use simulations to evaluate the resilience to packet loss and modifiers. The metric here is the verification rate, i.e., the ratio of number of authenticated packets to the number of received packets.

Node categorization is a perfect resilience to packet loss and intruders because of its inherent design. While it is not designed for lossy channels, it can also achieve the perfect resilience to packet loss in lossy channels.

In the lossy channel model where no Dos attack is assumed to present, we can set the threshold t=1 during transmission and thus each receiver can start batch verification as long as there is at least 1 packet received for each set of packets .

3.2. Efficiency

We consider latency, computation and communication overhead for efficiency evaluation under lossy channels and Dos channels.

3.3. Dos resilience

The signing and verification time is less. The signing is efficient. Therefore, we can save more computation resource at the sender.

It can achieve more bandwidth efficiency by using node categorization. It can generate smaller key length.

4. RELATED WORKS

The approaches for detecting packet dropping attacks can be categorized as three classes: multipath forwarding approach, neighbor monitoring approach, and acknowledgment approach. Multipath forwarding [3], [13] 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 watchdog method was originally proposed to mitigate routing misbehavior in mobile ad hoc networks [14]. It is then adopted to identify packet droppers in wireless sensor network. When the watchdog mechanism is deployed, each node monitors its neighborhood collect the firsthand information on its neighbor nodes. A variety of reputation systems have been designed by exchanging each node's firsthand observations, which are further used to quantify node's reputation. Based on the monitoring mechanism, the intrusion detection systems are proposed however, the watchdog method requires nodes to buffer the packets and operate in the promiscuous mode, the storage overhead and energy consumption may not be affordable for sensor nodes. In addition, this on the bidirectional communication links; it may not be effective when directional antennas are used. Particularly, this approach cannot be applied when a node does not know the expected output of its next hop since the node has no way to find a match for buffered packets and overheard packets. Note that, this scenario is not rare, for example, the packets may be processed, and then encrypted by the next hop node in many applications that security is required. Since the watchdog is a critical component of reputation systems, the limitations of the watchdog mechanism can also limit the reputation system. Besides, a reputation system itself may become the attacking target. It may either be vulnerable to bad mouthing attack or false praise attack. The third approach to deal with packet dropping attack is the multihop acknowledgment technique [9]. By obtaining responses from intermediate nodes, alarms, and detection of selective forwarding attacks can be conducted. To deal with packet modifiers, most of existing countermeasures are to modified messages within a certain number of hops so that energy will not be wasted to transmit modified messages. The effectiveness to detect malicious packet droppers and modifiers is limited without identifying them and excluding them from the network. Researchers hence have proposed schemes to localize and identify packet droppers, one approach is the acknowledgment-based scheme [10][11] for identifying the problematic communication links. It can deterministically localize links of malicious nodes if every node reports ACK using onion report. However, this incurs large communication and storage overhead for sensor networks. The probabilistic ACK approaches are then proposed in [14] and [15], which seek tradeoffs among detection rate, communication overhead, and storage overhead. However, these approaches assume the packet sources are trustable, which may not be valid in sensor networks. As in sensor networks, base station typically is the only one we can trust. Furthermore, these schemes require setting up pair wise keys among regular sensor nodes so as to verify the authenticity of ACK packets, which may cause considerable overhead for key management in sensor networks [12 -13]. Ye et al. [15] proposed a scheme called PNM for identifying packet modifiers probabilistically. However, the PNM scheme cannot be used together with the false packet filtering schemes .Because the filtering schemes will drop the modified packets which should be used by the PNM scheme as evidences to infer packet modifiers. This degrades the efficiency of deploying the PNM scheme.

5. CONCLUSION

In our work can effectively find out the intruders both packet droppers and packet modifiers than previous algorithms by using our effective node categorization and global ranking algorithms .Both algorithms runs in the base station and fully monitor the incoming packets. In our work network structure is not static; it is changed at every round interval. The node categorization algorithm executes after every round finished and remove the bad nodes from the network based on the packet marks. And global ranking algorithm executes after certain round finished this algorithm takes the previous round result and then remove the suspiciously bad nodes from the network.

REFERENCES

1.  Ayyaswamy Kathirvel and Rengaramanujam Srinivasan, "ETUS: Enhanced Triple Umpiring System for Security and Robustness of Wireless Mobile Ad Hoc Networks", International Journal of Communication Networks and Distributed Systems, Vol. 7, No. 1 / 2, pp. 153 – 187, 2011.
2.  Ayyaswamy Kathirvel and Rengaramanujam Srinivasan, "ETUS: An Enhanced Triple Umpiring System for Security and Performance Improvement of Mobile Ad Hoc Networks", International Journal of Network Management, Vol. 21, No. 5, pp. 341 – 359, 2011.
3. S.E. Deering, "Multicast Routing in Internetworks and Extended LANs," *Proc. ACM SIGCOMM Symp. Comm. Architectures and Protocols*, pp. 55-64, Aug. 1988.
4. T. Ballardie and J. Crowcroft, "Multicast-Specific Security Threats and Counter-Measures," *Proc. Second Ann. Network and Distributed System Security Symp. (NDSS '95)*, pp. 2-16, Feb. 1995.
5. Yun Zhou, Xiaoyan Zhu, Yuguang Fang, "MABS: Multicast Authentication Based on Batch Signature," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 982-993, July 2010.
6. J. Jeong, Y. Park, and Y. Cho, "Efficient DoS Resistant Multicast Authentication Schemes," Proc. Int'l Conf. Computational Science and Its Applications", 2005, pp.353-362.
7. A. Perrig, R. Canetti, J.D. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels", *Proc. IEEE Symp. Security and Privacy (SP '00)*, pp. 56-75, May 2000.
8. S. Miner and J. Staddon, "Graph-Based Authentication of Digital Streams," *Proc. IEEE Symp. Security and Privacy (SP '01)*, pp. 232-246, May 2001.
9. N. Koblitz, "Elliptic Curve Cryptosystems," *Math. Computation*, vol. 48, pp. 203-209, 1987.
10. M. Kefayati, H.R. Rabiee, S.G. Miremadi, and A. Khonsari,"Misbehavior Resilient Multi-Path Data Transmission in Mobile Ad-Hoc Networks", Proceedings of the fourth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '06), 2006.
11. 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.
12.  Selvaraj Navaneethan Identify Suspect Nodes in Selective Forwarding Attacks," Journal Parallel and Distributed Computing, Vol. 67, No. 11, 2015.
13.  Selvaraj navaneethan "Packet- Dropping Adversary Identification for Data Plane Security", Proc. ACM CONEXT Conf. (CoNEXT '08), 2008.

