International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Secure Data Transmission in Wireless Sensor Networks : Against Packet Dropping Attacks

Gonugunta Tulasi, R.Suresh, Professor

Gonugunta Tulasi, PG Scholar, Dept. of CSE, CREC, Tirupati, AP, India
R.Suresh, .Professor, Dept. of CSE, CREC, Tirupati, AP, India

Abstract: Wireless sensor network increases its application in industrial field as well as in consumer application very rapidly. Its growth increases day by day. Sensor node normally senses the physical event from the environment such as temperature, sound, vibration, pressure etc. Sensor nodes are connected with each other through wireless medium such as infrared or radio waves it depends on applications. Each node has its internal memory to store the information regarding the event packets. Basically this whole sensor network called sensor net is working in a distributive manner, sensor nodes are deployed in a huge area and use to send data packet in broadcast manner. This data packet finally reaches to the base station or called sink and vice versa. Nodes are deployed over a huge region in an ad-hoc based manner and use to sense the physical events. If any region cannot be sensed by any nodes then that region is called blind area. If blind area is too large then data retrieval is become unreliable. Nodes normally works in a collaborative manner to perform a specific task by transferring data packet to its neighbor nodes and so on until it reached to the base station. Every node has its own transmission range and within this transmission range node can transmit data packet. The event packet which sensor node transmit may be secret or confidential for the application , so the data transmission must be secured to maintain the confidentiality of data packets.

Keywords: Packet dropping, secure routing, attack detection, Packet Modification, Wireless Sensor Networks.

I. INTRODUCTION

packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multi hop sensor networks Many schemes have been proposed to mitigate and reduce such attacks, but very few can effectively and efficiently identify the intruders For packet drop widely used countermeasure is multipath forwarding[2],[3],[4],[5] in which data packets are forwarded in multiple paths and hence packet dropping though not in all paths but could be reduced to a considerable extent To deal with packet modification, the popularly used method is to track the hops for modified packets and to filter them These methods though deal with packet modification and drop but the threat of intruder has not been answered To address these problem, we propose a simple yet effective scheme, which can identify misbehaving forwarding nodes that drop or modify packets by continuously monitoring the behaviours of the nodes in the networks [10]

II. THE PROPOSED SCHEME

Our proposed scheme contains three techniques

A. Node Monitoring:

To locate and identify packet droppers and modifiers, it has been proposed that nodes are continuously monitored for forwarding behaviors and reputation [Bad and suspiciously Bad] of every node is published among the network and maintained in Central node [Sink].

B.PacketSealing:

In this scheme, when the sensor data are transmitted by nodes to sink, each packet sender or forwarder seals the data by adding a small number of extra bits called packet seals, from which sink could obtain useful data related to the transmission. Based on the packet seals, the sink can figure out the dropping ratio of every sensor node.

C.Node Classification:

The sink identifies and classifies the nodes that are droppers modifiers. The behaviour of nodes are traced in variety of scenarios and with the information accumulated in sink, it classifies the nodes as droppers /modifiers for sure or suspicious droppers /modifiers.

III. SYSTEM MODEL

A. Network assumptions:

The deployment of sensor networks could be such where a large number of sensor nodes are randomly deployed in a two dimensional area. each sensor node generates sensory data periodically and all these nodes collaborate to forward packets containing the data toward a sink. the sink is located within the network. we assume all sensor nodes and the sink are loosely time synchronized , which is required by many applications. attack resilient time synchronization schemes, which have been widely investigated in wireless sensor networks can be employed. the sink is aware of the network topology, which can be achieved by requiring nodes to report their neighboring nodes right after deployment.

B.SecurityAssumption:

The network sink is trustworthy and free of compromise, and the adversary cannot successfully compromise regular sensor nodes during the short and changing topology establishment after the network deployment. this assumption has been widely made in existing work [8].

IV. IMPLEMENTATION MODEL

In the implementation phase, sensor nodes form a topology which is a directed graph (DG). A routing tree is formed using directed graph. Data flows follow the routing tree structure. In each round, data are transferred through the routing tree to the sink. Each packet sender/forwarder adds a small number of extra bits to the packet (Packet seal) and also encrypts the packet. When one round finishes, based on the extra bits carried in the received packets, the sink runs a node classification algorithm to identify nodes that must be bad(i.e., packet droppers or modifiers) and nodes that are suspiciously bad (i.e., suspected to be packet droppers and modifiers). The routing tree is reshaped every round. As a certain number of rounds have passed, the sink will collect information about node behaviors in different routing topologies. The information includes which nodes are bad for sure, which nodes are suspiciously bad, and the nodes' topological relationship. The implementation is done in a sequential manner, we first present the algorithm for DG establishment and packet transmission, which is followed by the proposed categorization algorithm, tree structure reshaping algorithm, and heuristic ranking algorithms. To ease the presentation, we first concentrate on packet droppers and assume no node collusion. After that, we present how to extend the presented scheme to handle node collusion and detect packet modifiers, respectively.

A. DG Establishment and Packet Transmission

All sensor nodes form a DG and extract a routing tree from the DG. The sink knows the DG and the routing tree, and shares a unique key with each node. When a node wants to send a packet, it attaches to the packet a sequence number, encrypts the packet only with the key shared with the sink, and then forwards the packet to its parent on the routing tree. When an intermediate node receives a packet, it attaches a few bits to the packet to mark the forwarding path of the packet, encrypts the packet, and then forwards the packet to its parent. On the contrary,
a misbehaving intermediate node may drop a packet it receives. On receiving a packet, the sink decrypts it, and thus finds out the original sender and the packet sequence number. The sink tracks the sequence numbers of received packets for every node, and for every certain time interval, which we call a round, it calculates the packet dropping ratio for every node. Based on the dropping ratio and the knowledge of the topology, the sink identifies packet droppers.

B. Node Classification Algorithm

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, 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. The dropping ratio in this round is calculated as follows the tree topology, the sink identifies the nodes that are droppers for sure and that are possibly droppers. After then, for each path from a leaf node to the sink, the nodes' mark pattern in this path can be decomposed into any combination of the following basic patterns, which are also illustrated by Fig. 1:

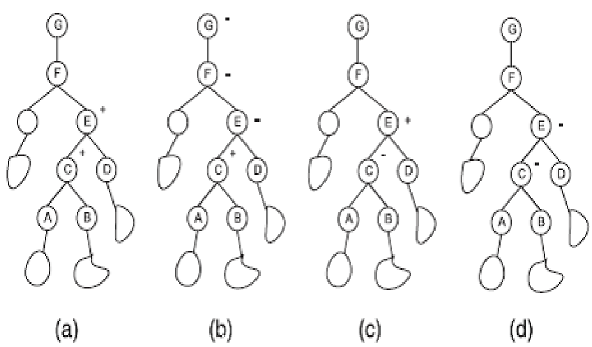

Fig 1: Node Status Pattern

V. RELATED WORK

The approaches for detecting packet dropping attacks can be categorized as three classes: multipath forwarding approach, neighbour monitoring approach, and acknowledgment approach. Multipath forwarding [4], [5] is a widely adopted countermeasure to mitigate packet droppers, which is based on delivering redundant packets along multiple paths. Another approach is to take up the monitoring mechanism .

can be conducted. To deal with packet modifiers, most of existing countermeasures [6], [7], [8], [9] are to filter 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 one approach is the acknowledgment-based 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 which seek trade-offs 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 to set up pairwise 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.

VI. CONCLUSION

The proposed scheme is effective to identify misbehaving forwarders that drop or modify packets. Each packet is encrypted and sealed so as to hide the source of the packet. The packet seal, 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 behaviours of sensor nodes can be observed in a large variety of scenarios and most of the bad nodes can be identified Extensive analysis, simulations, and 008 implementation have been conducted and verified the effectiveness of the proposed scheme.

ACKNOWLEDGMENT

The proposed work has been simulated in NS-2 and still working to get efficient results in avoiding and detecting intrusion in Wireless sensor networks.

VII.REFERENCES

[1] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks,"
Computer, vol. 36, no. 10, pp. 103-
105, Oct. 2003.
[2] C. Karlof and D. Wagneas r, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003.
[3] V. Bhuse, A. Gupta, and L. Lilien, "DPDSN: Detection of Packet- Dropping Attacks for Wireless Sensor Networks," Proc. Fourth Trusted Internet Workshop, 2005.

[4] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] Z. Yu and Y. Guan, "A Dynamic En-route Scheme for Filtering False Data in Wireless Sensor Networks," Proc. IEEE INFOCOM,2006.

[10] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, 2000. [11] M. Just, E. Kranakis, and T. Wan, "Resisting Malicious Packet Dropping in wireless Ad Hoc Networks," Proc. Int'l Conf. Ad-Hoc Networks and Wireless ADHOCNOW '03), 2003.

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

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

[14] 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), 2.