International Journal of Wireless Communication and Simulation
ISSN 2231-1254 Volume 5, Number 1 (2013), pp. 41-48

https://dx.doi.org/10.37622/IJWCS/5.1.2013.41-48□□

Detecting Packet Droppers and Modifiers in Wireless Sensor Networks

Raji P. and Mrs. Shobha Rani A.

M.Tech in Digital Communication Engineering

Associate Professor, Dept. of Electronics and Communication
Acharya Institute of Technology, Bangalore

Abstract

Wireless sensor networks have a wide range of applications in military and civilian domains.Wireless sensor networks are prone to attacks as they are usually deployed in a hostile environment. Packet dropping and modification are the common attacks that can be launched by an adversary to disrupt communication. In this paper, a scheme is proposed to efficiently detect packet droppers and modifiers. The sensor nodes are secured using distributed key generation mechanism. Depending upon the packet dropping, nodes are categorized as bad nodes and suspiciously bad nodes. Simulation of the proposed scheme is done using NS2 and effectiveness of the scheme is verified.

Keywords: sink, attacks, wireless sensor networks, packets, algorithm

INTRODUCTION

WSN technologies areused for a variety of applications. Typical applicationareas of wsn's include environmental, military, andcommercial enterprises. The rapid deployment, self-organization and fault tolerance characteristics of wireless sensor networks led to them being used as the sensing technology for military applications. The low cost and dense deployment characteristics make long system lifetime possible in a hostile environment-the enemies' destruction of a certain amount of WSN nodes does not cause as much harm as a traditional wiredsensor network.In underwater, sensor nodes forming anetwork could be used for oceanographic datacollection, pollution monitoring, assisted navigation, militarysurveillance, and mine reconnaissance operations. Futureimprovements in technology will bring more

sensorapplications into our daily lives and the use of sensors willalso evolve from merely capturing data to a system that canbe used for real-time compound event alerting.

Wireless sensor networks consist of alarge number of nodes which communicates through wireless medium and works cooperatively to sense or monitor the environment. Each sensor node consists of a radio transceiver for communication purposes, microcontroller for processing capabilities, a sensor for sensing or monitoring and battery for providing energy. The node senses data from environment and sends this data cooperatively to the sink/gateway node. The characteristics of wireless sensor nodes are that they are resource constrained and are deployed in unattended and unprotected environment. So they are vulnerable to attacks. 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. In this paper, an effective scheme is proposed to catch both packet droppers and modifiers.

RELATED WORK

To deal with packet droppers, a widely adopted countermeasure is multi-path forwarding [2], [3], [4], [5], in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated. DPDSN (Detection of Packet Dropping attacks for wireless Sensor Networks) [3], uses multipath routing.

In [7], Marti et al proposed a way of detecting malicious nodes through overhearing the next node's transmissions. They introduced the concept of watchdog and pathrater.

For packet modification the existing systems aim to filter modified messages en-route within a certain number of hops [8], [9], [10]. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught.

Filtering techniques are used in several methods, such as SAVE [9] and Hop-by-hop Authentication [10]. These approaches are of less utility against non-spoofed traffic. In addition, these schemes rely upon some way of distinguishing attack packets from legitimate ones.

To locate and identify packet droppers and modifiers, it has been proposed that nodes continuously monitor the forwarding behaviours of their neighbours [11], [12] to determine if their neighbours are misbehaving, and the approach can be extended by using the reputation-based mechanisms to allow nodes to infer whether a non-neighbour node is trustable.

M. Just et al [11] present a proactive distributed probing protocol to detect and mitigate the malicious packet dropping attacks. In their approach, every node proactively monitors the packet forwarding behaviour of the others by mixing probing messages into the usual traffic. The probing messages look indistinguishable from normal packets, and they may be piggybacked on regular packets. A node infers the

legitimacy of its neighbour from the received acknowledgments in response to the probes. In their protocol, the probing packet anonymity is achieved through packet encryption.

Ye et al. proposed a probabilistic nested marking (PNM) scheme [13]. But with the PNM scheme, modified packets should not be filtered out en route because they should be used as evidence to infer packet modifiers; hence, it cannot be used together with existing packet filtering schemes. Since these approaches have several drawbacks like incompatibility with existing systems, high energy cost etc., our proposed work can be used to overcome these constraints.

NETWORK ASSUMPTIONS

Consider a typical deployment of sensor networks, 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. The network sink is trustworthy and free of compromise and the adversary cannot successfully compromise regular sensor nodes during the short topology establishment phase after the network is deployed. A compromised node can launch two types of attacks, packet dropping and packet modification.

PROPOSED SCHEME

The framework consists of three modules: System initialization, Crypto forwarding and Ranking algorithm. In the system initialization phase, network topology is established and keys are distributed among the network. The nodes can communicate securely within the network by knowing their corresponding IDs. This is used by the nodes as key for encryption of data. Each packet sender/forwarder adds a small number of extra bits to the packets and encrypts the packet. Depending on the dropping ratio of each sensor nodes, sink categorizes node as dropping node or suspiciously bad node.

System initialization

Topology is established between sensor nodes with sink. Sink provides the key to all nodes within the networkshares of the key generationmaterial that would be given to each of the initial set ofnodes before deployment. The shares should have theproperty that no set of nodes less than or equal to *t* shouldbe able to generate either the coefficient matrix A, or thevector X^TA for any other node.

Each node that is deployed would be initialized with amatrix Ai where Ai is of the following form:

$$\begin{pmatrix} s_{00} & \cdots & S_{0t} \\ \vdots & \ddots & \vdots \\ s_{t0} & \cdots & s_{tt} \end{pmatrix}$$

Each elementsijis given by:

$$s_{ij} = a_{ij} + \sum_{m=1}^{t1} b_{ijm}(\beta^m) \quad (1)$$

Here*bijm*are random numbers generated by the sink. These numbers are not known to anyone except the sink.*t1*is the threshold for sharing thematrixA. β is the ID of the node.

In this scheme, sensor nodes communicate with other nodes just by knowing their correspondingIDs.

The bivariate polynomials are shared in such amanner that the shares depend on the coefficient matrix of the polynomial, the requesting node's ID and the ID of the nodes that respond to the request.

Crypto Forwarding module

Each node maintains a counter which keeps track of the number of packets that it has sent. When a sensor node u has a data item to report, it composes and sends the packet to its parent node: It sends following bits, the sequence number of the packet. Data is encrypted using the key, arandom number picked by node u. Paddings are added to make all packets equal in length.

After encrypting the data using the key, it is forwarded to the intermediate nodes. The intermediate node chops off some of the bits and adds some extra bits so that the sink can identify which node has sent the data.

In this scenario it is difficult for a node to be attacked as it is difficult to find the key. Comprising a node does not enable the attacker to find the key as it is distributed among nodes.

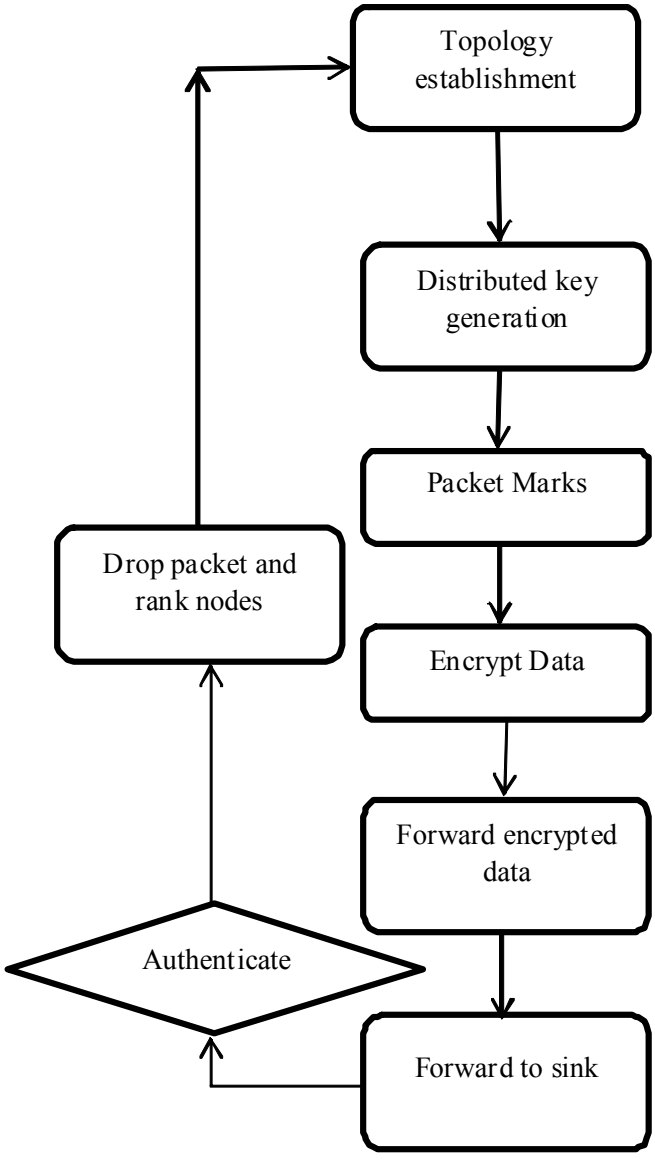
At last the intermediate node forwards the data to the sink. The sink receives all packets from the sender nodes. Sink decrypts the packet using the key. If it fails to decrypt the packet, the packet is considered to be modified and the packet is dropped. Once all packets are decrypted it is merged to get the original file.

Ranking algorithm

In this module, nodes will be categorized as good nodes, bad nodes and suspiciously bad nodes depending on the node behaviour. The dropping ratio of each node helps to find out whether a node is good or bad. The number of times a node drops packet is considered to rank each node.

SYSTEM DIAGRAM

An activity diagram shows the flows from activity to activity within a system. They address the dynamic view of a system.



TOPOLOGY

The simulation of the network is done using network simulator ns-2.34. The numbers of nodes is varied from 50 to 200 and are randomly deployed in an area of 3000 x 1000 square meters. Simulation time is 100 seconds. Figure shows animation capture of a network of 50 nodes.

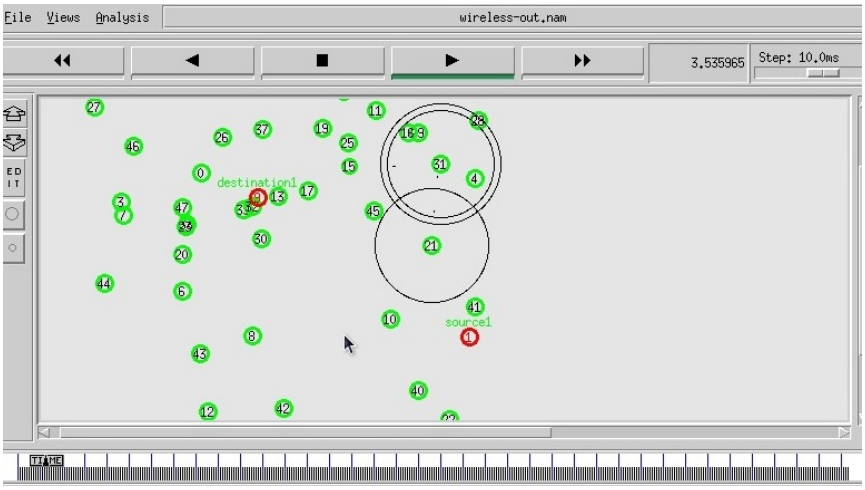


Figure2. Topology of WSN

The network is analysed for different number of sensor nodes and malicious nodes. The malicious nodes are identified considering different sources and destinations.

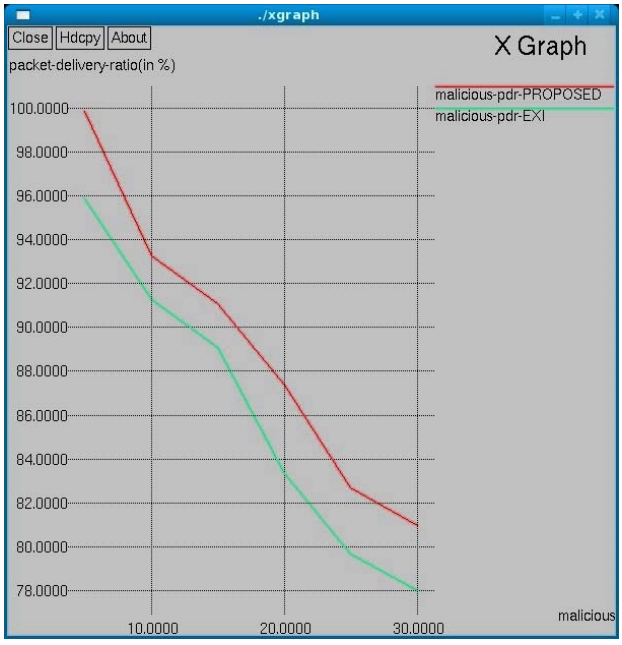


Figure 3. Packet delivery ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.Packet delivery ratio and routing overhead is calculated and depicted in the graphs in Figures 3 and 4.

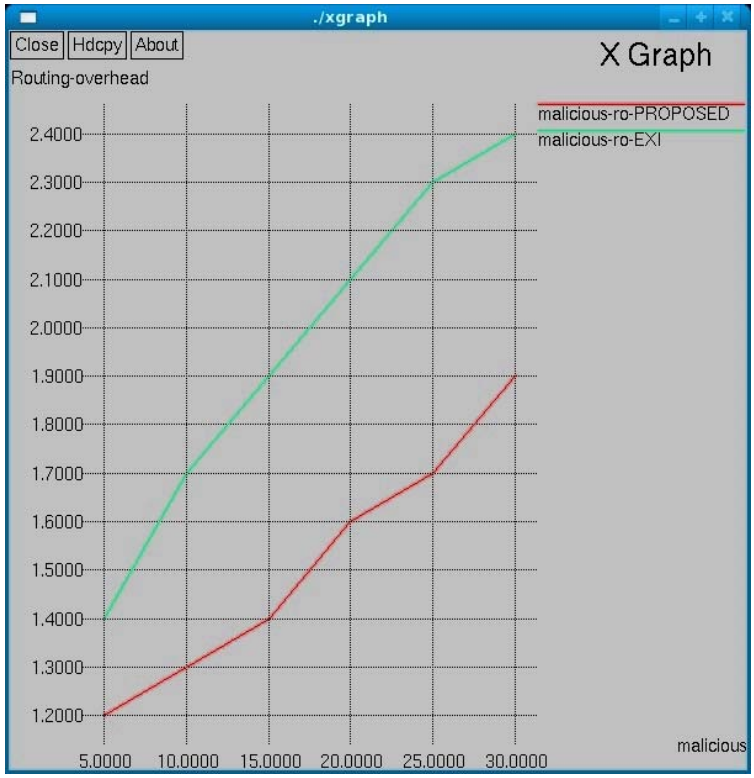


Figure 4. Routing overhead

CONCLUSION

In this paper, efficient and secure communicationframeworks have been developed for WSN applications. Security features have been incorporated into the network using distributed key generation mechanism. The scheme has been evaluated using the simulator and results are compared under attack with and without the scheme. The results show a significant increase in false detection ratio and increase in packet delivery ratio. Thus, the system successfully defends the attack and detects packet modifiers and droppers.

REFERENCES

[1] Chuang Wang, TaimingFeng, Jinsook Kim, Guiling Wang, and Wensheng Zhang, “Catching Packet droppers and modifiers in wireless sensor networks, ” IEEE transactions on parallel and distributed systems, vol. 23, no. 5, may 2012.

[2] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures, ” in the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[3] V. Bhuse, A. Gupta, and L. Lilien, "Dpdsn: Detection of packet-dropping attacks for wireless sensor networks, " in the 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, " in ACM SASN, 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, 2007.

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

[7] S. Marti, T.J. Giuli, K. Lai, and M. Baker."Mitigating routing misbehavior in mobile ad hoc networks". In Proc. 6th Annual International Conference on Mobile Computing and Networking, pages 255–265, 2000

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

[9] J. Li, J. Mirkovic, and M. Wang. "Save: Source Address Validity Enforcement Protocol".In Proc. IEEE INFOCOM 2002.

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

[11] M. Just, E. Kranakis, and T. Wan, "Resisting malicious packet dropping in wireless ad hoc networks, " in ADHOCNOW, 2003, vol. 2856.

[12] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks, " in IEEE CCNC, 2006.

[13] F. Ye, H. Yang, and Z. Liu, "Catching Moles in Sensor Networks, " in IEEE ICDCS, 2007.

[14] Stephan Olariu, "*Information assurance in wireless sensor networks*", Sensor network research group, Old Dominion University.

[15] J. Zheng and Myung J. Lee (2006). A comprehensive performance study of IEEE 802.15.4 – Sensor Network Operations: Wiley Interscience. IEEE Press Chapter 4.218-237.