ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

Detection and Avoidance of Intrusion, Packet Drop and Modification in WSN

S.Sivanantham[1], K.Kirankumar[2],V. Akshaya[3]

Assistant professor, Department of I.T, Adhiyamaan college of Engineering, Hosur, India [1]

Assistant professor, Department of I.T, Adhiyamaan college of Engineering, Hosur, India [2]

Department of computer science, PMC Tech, Hosur, India [3]

Abstract: Wireless sensor network is deployed and operated in an unattended and hostile environment to monitor events , produce and transmit data. Nodes in the sensor network could be a gateway, base station, storage node, or querying user. Because of the ease of deployment, the low cost of sensor nodes and the capability of self-organization, sensor network is often used to perform monitoring and data collection tasks. Wireless sensors networks finds its major applications in Military and defence networks . When it is 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 [1] to disrupt the inter-network communication.

Keywords: Intrusion, Packet Drop, 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], [11], [12], [13], [14], [15].

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 behaviours and reputation [Bad and suspiciously Bad] of every node is published among the network and maintained in Central node [Sink].

B. Packet Sealing:

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 [21], which is required by many applications. attack resilient time synchronization schemes, which have been widely investigated in wireless

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

sensor networks [22], [23], can be employed. the sink is aware of the network topology, which can be achieved by requiring nodes to report their neighbouring nodes right after deployment.

Extensive simulation on ns-2 simulator has been conducted to verify the effectiveness and efficiency of the proposed scheme in various scenarios.

B. Security Assumptions:

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], [24].

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 behaviours 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:

$$\mathrm{d} = \frac{nu, flip * Ns + nu, max + 1 - nu, rcv}{nu, flip * Ns + nu, max + 1}$$

Based on the dropping ratio of every sensor node and 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:

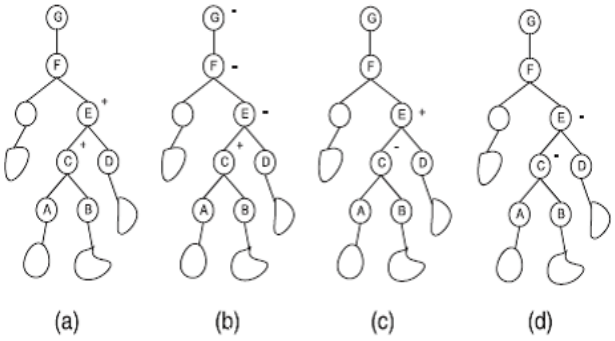

Fig.1. Node Status Pattern

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

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 [10], [13], [14], [16], [17], [18], [19], [27].

A variety of reputation systems have been designed by exchanging each node's first hand observations, which are further used to quantify node's reputation [16], [17], [18], [19]. Based on the monitoring mechanism, the intrusion detection systems are proposed in [15] and [29].

The third approach to deal with packet dropping attack is the multi hop acknowledgment technique [31], [32], [33]. By obtaining responses from intermediate nodes, alarms, and detection of selective forwarding

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 scheme [24], [25], [34] 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 [24] and [25], 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 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.

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), 2008.

[15] I. Krontiris, T. Giannetsos, and T. Dimitriou, "LIDeA: A Distributed Lightweight Intrusion Detection Architecture for Sensor Networks," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm '08), 2008.

[16] S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37, 2008.

[17] W. Li, A. Joshi, and T. Finin, "Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-Dimensional Trust Management Approach," Proc. 11th Int'l Conf. Mobile Data Management (MDM '10), 2010.

[18] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm.and Multimedia Security: Advanced Comm. and Multimedia Security, 2002.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

[19] S. Buchegger and J. Le Boudec, "Performance Analysis of the Confidant Protocol," Proc. ACM MobiHoc, 2002.
[20] F. Ye, H. Yang, and Z. Liu, "Catching Moles in Sensor Networks,"Proc. 27th Int'l Conf. Distributed Computing Systems (ICDCS '07),2007.
[21] Q. Li and D. Rus, "Global Clock Synchronization in Sensor Networks," Proc. IEEE INFOCOM, 2004.
[22] K. Sun, P. Ning, C. Wang, A. Liu, and Y. Zhou, "Tinysersync:Secure and Resilient Time Synchronization in Wireless Sensor Networks," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.
[23] H. Song, S. Zhu, and G. Cao, "Attack-Resilient Time Synchronization for Wireless Sensor Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 112-125, 2007.
[24] B. Xiao, B. Yu, and C. Gao, "Chemas: Identify Suspect Nodes in Selective Forwarding Attacks," J. Parallel and Distributed Computing, vol. 67, no. 11, pp. 1218-1230, 2007.
[25] X. Zhang, A. Jain, and A. Perrig, "Packet-Dropping Adversary Identification for Data Plane Security," Proc. ACM CONEXT Conf. (CoNEXT '08), 2008.842 IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012
[26] Crossbow, "Wireless Sensor Networks," http://www.xbow.com/Products/Wireless_Sensor_Networks.htm, 2011.
[27] T.H. Hai and E.N. Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-Hops Neighbor Knowledge," Proc. IEEE Seventh Int'l Symp. Network Computing and Applications (NCA '08), 2008.
[28] F. Liu, X. Cheng, and D. Chen, "Insider Attacker Detection in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2007.
[29] K. Ioannis, T. Dimitriou, and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks," Proc. 13th European Wireless Conf., 2007.
[30] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks," Proc. Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, 2008

BIOGRAPHIES

Sivanantham.S received his B.E in Department of Information Technology in Annamalai University in 2009 and received M.E in Department of Computer science in Annamalai University in 2011 and currently working as Assistant Professor in Department of I.T in Adhiyamaan college of Engineering Hosur.

Kirankumar.K received his B.E in Department of Computer science in Anna University in 2011 and received M.E in Department of Computer science in Anna University in 2013 and currently working as Assistant Professor in Department of I.T in Adhiyamaan college of Engineering Hosur.

Akshaya.V received her B.E in Department of Computer science in Anna University in 2012 and pursuing M.E in Department of Computer science in PMC Tech College, Hosur.