Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.92 – 96

RESEARCH ARTICLE

Effective Identification of the Intruders and Modifiers in Wireless Sensor Networks

J. Vijayagajendiran[1], D. Udhayakumarapandian[2]

[1]M. Tech student, Department of Computer Science and Engineering, Bharath University, India

[2]Assistant Professor, Department of Computer Science and Engineering, Bharath University, India

Abstract— Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multihop sensor networks. Many schemes have been 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, which can identify misbehaving forwarders that drop or modify packets. In Wireless Sensor Network, sensors at different locations can generate streaming/ discrete data, which can be analyzed in real-time/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. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. 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. As the tree structure dynamically changes every time interval, behaviors of sensor nodes can be observed in a large variety of scenarios. The information of node behaviors has been accumulated. Secondly, the sink will periodically run heuristic ranking algorithms to identify most likely bad nodes from suspiciously bad nodes. And an extension to identify modified packets using Message Authentication Code.

Key Terms: - wireless sensor networks; attacks; packet droppers; packet modifiers; message authentication code

I. INTRODUCTION

Wireless sensor network, 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. Because of the ease of deployment, the low cost of sensor nodes and the capability of self-organization, a sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. Wireless Sensor networks consist of large number of small sensor nodes having limited computation capacity, restricted memory space, limited power resource, and short-rage radio communication device. With a widespread deployment of these devices, one can precisely monitor the environment. Basically, sensor networks 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. A sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks.

Existing solution for detecting packet dropping in Wireless Sensor Networks is multipath forwarding [2], [3], [4], [5], in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all paths of these paths can be tolerated. And for detecting packet modifiers, most of existing

countermeasure [6], [7], [8], [9] aim to filter modified message en-route within a certain number of hops. 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.

In this paper, a simple yet effective scheme is proposed to catch both packet droppers and modifiers. In this scheme, first a routing tree is rooted at the sink. The 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 markers, to the packet. The format of the small packet marks is intentionally 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. Secondly, sink runs 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 large variety of scenarios. Finally, as the information of node behaviors has been accumulated, the sink periodically runs the proposed heuristic ranking algorithms to identify most likely bad nodes can be gradually identified with small false positive.

The proposed scheme is effective in identifying both packet droppers and modifiers with low communication and energy overheads and being compatible with existing false packet filtering schemes; that is, it can be deployed together with existing false packet filtering schemes, and therefore it cannot only identify intruders but also filter modified packets immediately after the modifications is detected.

II. RELATED WORKS

There are three types of existing approaches to detect packet dropping attacks. They are multipath forwarding approach, neighbour monitoring approach, and acknowledgement 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 exploit the monitoring mechanism [10], [13], [14], [16], [17], [18], [19], [23]. The watchdog method was originally proposed to mitigate routing misbehavior in mobile ad hoc network [13], [23], [24]. When the watchdog mechanism is deployed, each node monitors its neighbourhood promiscuously to collect the first hand information on its neighbour nodes. A variety of reputation systems have been designed by exchanging each node's reputation [16], [17], [18], [19]. Based on the monitoring mechanism, the intrusion detection systems are proposed in [15] and [25]. 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 mechanism relies on the bidirectional communication links; this may not be effective when directional antennas are used [26]. 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 overhead 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 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 [26]. The third approach to deal with packet dropping attack is the multi hop acknowledgement technique [27], [28], [29].

By obtaining response from intermediate nodes, alarms, and detection of selective forwarding attacks can be conducted. 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 [21], [22], [30], 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 [21] and [22], 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 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. Ye et al. [20] proposed a scheme called PNM for identifying packet modifiers probabilistically. However, the PNM scheme cannot be used together with the false packet filtering schemes [6], [7], [8], [9], because the filtering schemes will drop the modified packets which should be used by the PNM scheme as evidence to infer packet modifiers. This degrades the efficiency of deploying the PNM scheme.

III. SYSTEM MODEL

3.1 Creation of Network Topology

In the initialization phase, sensor nodes form a topology which is a directed acyclic graph (DAG). A routing tree is extracted from the DAC .Data reports follow the routing tree structure. In each round, data are transferred through the routing tree to the sink. When a node wants to send out 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 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; the sink runs a node categorization algorithm to identify nodes that must be bad and suspiciously bad.

3.2 Initialization of Secret Pair wise Keys

After sensor nodes form a topology which is a directed acyclic graph (DAC), each sensor node u is preloaded with the following information

- Ku: a secret key exclusively shared between the node and the sink.
- Lr: the duration of a round.
- Np: the maximum number of parent nodes that each node records during the DAC establishment procedure.
- Ns: the maximum packet sequence number

3.3 Packet Sending and Forwarding

When a sensor node u has a data item D to report, it composes and sends the following packet to its parent Pu:
< Pu, {Ru, u, CpMODNs, D, padu,o }ku, padu,1>

Each node maintains a counter Cp which keeps track of the number of packets that it has sent so far. Where CpMODNs is the sequence number of the packet. Ru ($0 \leq Ru \leq Np-1$) is a random number picked by node u during the system initialization phase, and Ru is attached to the packet to enable the sink to find out the path along which the packet is forwarded, {X}y represents the result of encrypting X using key Y.

Padding padu, 0 and pad u, 1 are added to make all packets equal in length, such that forwarding nodes cannot tell packet sources based on packet length. Meanwhile, the sink can still decrypt the packet to find out the actual content. To satisfy these two objectives simultaneously, the paddings are constructed as follows:

For a packet sent by a node which is h hops away from the sink , the length of padu,1 is log(Np)*(h−1) bits. As to be described later, when a packet is forwarded for one hop, log (Np) bits information will be added and meanwhil, log (Np) bits will be chopped.

Let the maximum size of a packet be Lp bits, a node ID be Lid bits and data D be Ld bits, padu, 0 should be Lp−Lid*2−log (Np)*h−log (Ns) −Ld bits, where Lid*2 bits are for Pu and u fields in the packet, field Ru is log (Np) bits long, and Cp MOD Ns is log (Ns) bits long. Setting padu, 0 to this value ensures that all packets in the network have the same length Lp.

When a sensor node v receives packets <v, m>, it composes and forwards the following packet to its parent to its parent to its parent node Pv:
<Pv, {Rv, m} Kt>,

Where m' obtained by trimming the rightmost log (Np) bits off m. Meanwhile, Rv, which has log Np bits, is added to the front of m'. Hence, the size of the parent remains unchanged.

3.4 Packet Receiving at the Sink

We use node 0 to denote the sink. When the sink receives a packet <0, m'>, it conducts the following steps;

1. Initialization. Two temporary variables u and m are introduced. Let u=0 and m= m' initially.
2. The sink attempts to find out a child of node u, denoted as v, such that dec(Kv, m) results in a string starting with Rv, where dec(Kv, m) means the result of decrypting m with key Kv.
3. If the attempt fails for all children nodes of node u, the packet is identified as have been modified and thus should be dropped.

4. If the attempt succeeds, it indicates that the packet was forwarded from node v to node u. Now, there are two cases:
    - If dec (Kv, m) starts with < Rv, v>, it indicates that node v is the original sender of the packet is recorded for further calculation and the receipt procedure completes.
    - Otherwise, it indicates that node v is an intermediate forwarder of the packet. Then, u is updated to be v; m is updated to be the string obtained by trimming Rv from the leftmost. Then, steps 2-4 are repeated.

3.5 Categorization and Ranking Algorithm

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. For every round sink will keep track of these information and at the end of each round it will calculate the dropping ratio for each node u.

3.5.1 Identifying Bad Nodes from Suspiciously Bad Nodes

After each round, the sink calculates the dropping ratio of each node, and runs the categorization algorithm to identify nodes bad for sure and suspiciously bad. The Global Ranking-based (GR) method can detect most bad nodes with some false accusations while the Step-Wise Ranking based method has fewer false accusations but may not detect as man y bad nodes as the GR method. To obtain a balance, the Hybrid ranking-based (HR) method is used. In HR method, the node with the highest accused account value is still first chosen as most likely bad node. After a most likely bad node has been chosen, the one with the highest accused account value among the rest is chosen only if the node has not always been accused together with the bad nodes that have been identified already, thus the accusation value is considered as an important criterion in identification, as in the GR method.

IV. CONCLUSION

A simple effective scheme is proposed 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 sink can recover the source of the packet and then dropping ratio of each node is calculated. Finally bad nodes can be identified by heuristic ranking algorithm with small positive. Then modified packets will be dropped by honest nodes on the way to the sink using Message Authentication Code (MAC).

REFERENCES

[1] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, Member, IEEE, and Wensheng Zhang, Member "Catching Packet Droppers and Modifiers in Wireless Sensor Networks" in IEEE Trans on Parallel Distributed Systems, vol. 36, no. 5, May 2012.
[2] C. Karlof and D. Wagner, "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, "Misbehaviour Resilient Multi-Path Data Transmission in Mobile Ad-Hoc Networks," Proc. Frouth 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, vol. 5, no. 1, pp. 87-99, 2007.
[6] F. Ye, H. Luo, S.Lu, and L.Zhang, "Statistical En-Routing 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 AdHoc Networking and Computing (MobiHoc '05),2005.
[9] Z. Yu and Y. Guan, " A Dynamic En-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 Nodes in Sensor Networks," Proc. Frouth 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. Frouth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), 2008.
[15] I. Krontiris, T. Ginneetsos, and T. Dimitriou, "LIDeA: A Distributed Lightweigth Intrusion Detection Architecture for Sensor Networks," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (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 Misbehaviours 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.
[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] 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.
[22] X. Zhang, A. Jain, and A. Perrig, "Packet-Dropping Adversary Identification for Date Plane Security," Proc. ACM CONTEXT Conf. (CoNEXT '08), 2008.
[23] T.H. Hai and E.N. Huh, "Detecting Selective Forwarding Attacks in WirelessSensor Networks Using Two-Hops Neighbor knowledge," Proc. IEEE Seventh Int'l Symp. Network Computing and Applications (NCA '08), 2008.
[24] F. Liu, X. Cheng, and D. Chen, " Insider Attacker Detection in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2007.
[25] K. Ioannis, T. Dimitriou, and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks," Proc. 13th European Wireless Conf., 2007.
[26] 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.
[27] J.M. Mccune, E. Shi, A. Perrig, and M.K. Reiter, "Detection of Denial-of-Message Attacks on Sensor Network Broadcasts," Proc. IEEE Symp. Security and Policy, 2005.
[28] B. Yu and B.Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," Proc. 20th Int'l Symp. Parallel and Distributed Processsing (IPDPS), 2006.
[29] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, "An Acknowledgement-Based Approach for the Detection of Routing Misbehaviour in Manets," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.
[30] B. Barak, S. Goldberg, and D. Xiao, "Protocols and Lower Bounds for Failure Localization in the Internet," Proc. Eurocrypt, 2008.

