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. 3, Issue. 7, July 2014, pg.936 – 941

RESEARCH ARTICLE

Recognition of Packet Dropping and Modification in WSN's using Ranking Algorithms

M. Suresh[1], Sunil Kumar. V[2]

[1]M.Tech 2nd year, Department of CSE, PBR VITS, Kavali, Nellore, A.P, India

[2]Associate Professor, Department of CSE, PBR VITS, Kavali, Nellore, A.P, India

[1] suryamaramreddy@gmail.com; [2] sunil.vemula1981@gmail.com

Abstract- In wireless sensor networks the Packet Droppers and Modifiers are common attacks. It is very difficult to identify such attacks and this attack interrupts the communication in wireless multi hop sensor networks. In this we can identify the Packet Droppers and Packet Modifiers using ranking algorithms and packet marks. The Performance is represented using detection rate and false positive probability. So 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 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 this paper extensive analysis and simulations have been conducted to verify the effectiveness and efficiency of the scheme. The Proposed scheme provides an effective mechanism for catching compromised node.

Keywords- packet droppers and modifiers, intrusion detection, Routing, wireless sensor networks, Authentication Code, Compromised nodes

I. INTRODUCTION

The Simplicity in Wireless Sensor Network with resource constrained nodes makes them really vulnerable to variety of attacks. In a Wireless sensor networks sensor nodes monitor the environment, and detect events of interest, produce data and collaborate in forwarding the data towards to a sink, which could be a gateway, base station or storage node. Securing the Wireless Sensor Networks need to build the network support all security properties: integrity, confidentiality, authenticity and availability. A sensor network is often deploying 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. After compromising one or multiple sensor nodes, an adversary may launch a variety of 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.

We expect sensor networks to consist of hundreds or thousands of sensor nodes as in Fig 1. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who capture and reprogram individual sensor nodes. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the adversary can then increase a variety of attacks.

Packet dropping is nothing but a bad node drops all or some of the packets that are supposed to be forwarded. It may also drop the data generated by itself for some malicious purpose such as blaming innocent nodes. This paper proposes a scheme to catch both packet droppers and modifiers. At first routing tree is established using DAG. Data is transmitted along the tree structure toward the sink. A packet sender or forwarder adds a small number of extra bits, which is called packet marks, are designed such that the sink can obtain the dropping ratio associated with every sensor node. Node categorization algorithm to identify nodes that are dropper's modifiers for sure or are suspicious droppers/ modifiers [1].

Network Assumptions

In this network assumptions, we assume that a typical deployment of sensor network, as where a large number of sensor nodes are deployed in a two dimensional area. Each sensor node generates sensing data periodically and all these nodes collaborate to forward packets that contain the data hop by hop towards a sink. In this the sink is located at some place within the network. We assume that all sensor nodes and the sink are time synchronized, which is required by many applications. The sink is aware of the network topology, which can be achieved by requiring nodes to report their neighboring nodes soon after deployment.

Security Assumptions and Attack Model

We assume that the network sink is reliable and free of compromise, but regular sensor nodes can be compromised. Compromised nodes may or may not collude with each other. A compromised node can launch the following two attacks:

[1] **Packet dropping:** A compromised node drops all or some of the packets that it is supposed to forward. Here it may also drop the data generated by itself for some malicious purpose such as accusing innocent nodes.

[2] **Packet modification:** A compromised node modifies all or some of the packets that it is supposed to forward. So here it may also modify the data it generates to protect itself from being identified or to accuse other nodes.

II. RELATED WORK

There are several approaches made for detection of vulnerable attacks. [2][3][4][5][6] Deals with packet dropping. [2] Detection of packet dropping attacks for WSN proposes a solution to identify paths that drop packets by using alternate paths, but it succeeds only when the alternate path does not have any malicious nodes. [3] In this scheme single path data forwarding is employed and later it is convertor in multipath data forwarding. [4][5][6] are related to routing process and neighbour monitoring mechanism. [7][8] Deals with packet modification. [7] In this SEF detect and filters out false reports based on probabilistic key distribution. Proposes Location Based Resilient security to filter out packets, but in spite of all filtering techniques intruders are able to move on and communication overhead is increased. Probabilistic Nested marking is proposed to locate vulnerable nodes and it does so within the framework of packet marking, but the evidence to find packet modifiers are also filtered out. [9] In this paper extensions to Dynamic Source Routing are given such as watchdog and pathrater. Watchdog identifies misbehaving nodes and pathrater helps routing protocols avoid those nodes [10]. Few existing system deals with selective forwarding attacks which corrupt time critical application, to overcome this factor is proposed where checkpoint based multi hop acknowledgement scheme for detecting selecting forwarding attacks.

III. Packet Dropping and Modification in Wireless Sensor Networks

Existing counter measures aim to filter modified messages resend within a certain number of hopes. These measures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue the network without being caught. In existing scheme, modified packets should not be filtered out en route because they should be used as evidence to infer modified packets; hence, it cannot be used together with existing packet filtering schemes.

Disadvantages of Existing system:

- Intruders are able to collect the data while we are sending data from source to destination.
- It is not possible to send modified packets to destination.
- It cannot be easy to find what the dropped and modified packets are.
- In this system, the modified packets should not be filtered out.

IV. Packet Modification and Dropping in WSN's using Ranking Algorithms

4.1. Initialization phase:

In the initialization phase, sensor nodes form a topology which is direct acyclic graph (DAG).A routing tree is extracted from the DAG. Data reports follow the routing tree structure. The purpose of system initialization is to set up secret pair wise keys between the sink and every regular sensor node. To establish the

Each sensor node u is preloaded 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 DAG establishment procedure.
- Nsth packet is numbered Ns-1, the Ns-1th packet is numbered 0,and so on and so forth.
- Ns: the maximum packet sequence number.

4.2. Intruder Identification phase:

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 and also encrypts the packet. When one round finishes, based on the extra bits carried in the received packets, the sink runs a node categorization algorithm to identify nodes that must be bad nodes and suspiciously bad. The routing tree is reshaped every round, when a certain number of rounds have passed, sink collects enough information about node behaviors in different routing topologies.

4.3. Packet Sending:

When a sensor node u has a data item D to report, it composes and sends the following packet to its Node.

Pu: <Pu,{Ru,u,Cp MOD Ns,D,padu,0} Ku,padu,1>

Where Pu - parent node, Ru – receiving node, U- node, Cp – counter node, D – data ,pad u,0 –padding, Ku encryption. Puddings pad u,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.

4.4. Packet forwarding:

When a sensor node v receives packet hv;mi, it composes and forwards the following packets to its parent node Pv: $<P_{v,}\{R_{v,}m\}K_v>$

Where m is obtained by trimming the rightmost log (Np) bits off m. Meanwhile, Rv, which has logNp bits, is added to the front of m.

4.5. Packet receiving at the sink:

The sink attempts to find a child node for every parent node by decrypting which results in a string. If the attempt fails the packet is modified and it should be dropped. If it succeeds the packet is forwarded from the respective node.

4.6. Algorithm 1.Packet Receipt at the Sink

[1] Input: packet<0; m>.
[2] If Success Attempt =false then decrypt.

```
[3]  if decryption fails then continue, else
[4]  If Success Attempt=true then record sequence.
[5]  u←v, Success Attempt=false;go to line4.
[6]  if Success Attempt = false then
[7]  Drop this packet.
```

4.7. Algorithm 2. Tree-Based Node Categorization

```
1.  Input: Tree T, with each node u marked by "+" or"_," and its dropping ratio du.
2.  For each leaf node u in T find parent node until the sink node categorize the nodes.
3.  Consider u as positive threshold and v as negative threshold.
4.  If v. mark ="_"then until v.mark="+" or v is Sink,Set nodes from b to e bad for sure.
5.  If v is Sink then set u as bad for sure.
6.  If v. mark ="+" and if v is not bad for sure then set u and v as suspiciously bad else
7.  if $dv – du > \theta$ then
8.  Set v as bad for sure.
9.  if difference $du-dv > \theta$then Set u and v as suspiciously bad;
```

Nu,max - most recently seen sequence number
Nu,flip - the number of sequence number flips
nu,rcv - number of received packets.
The dropping ratio in each round is calculated as follows:

$$D_u = \frac{Nu,flip*Ns+Nu.max+1-nu.rc}{Nu,flip*Ns+Nu.max+1}$$

To identify most likely bad nodes from suspicious nodes:

$S_i = \{ < u_j,v_j > \mid < u_j,v_j > \text{ is a suspicious pair and } < u_j, v_j > = < u_j, v_j > \}$

Ranking Algorithms:

1. Global ranking based approach:

The GR method is based on the heuristic that, the more times a node is identified as suspiciously bad, the more likely it is a bad node. The node with the highest value is chosen as a most likely bad node and all the pairs that contain this node are removed.

2. Stepwise ranking based approach:

It can be anticipated that the GR method will falsely accuse innocent nodes that frequently been parents or children of bad nodes. Once a bad node u is identified, for any other node v that has been suspected together with node u, the value of node v's accused account is reduced by the times that u and v have been suspected together.

3. Hybrid Ranking-Based (HR) Method:

The GR Method can detect most bad nodes with some false accusations while the SR method has fever false accusations but may not detect as many bad nodes as the GR method. 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.

4. Packet Modifiers:

Modified packets can be detected with the afore-described scheme. Modified packets will be detected by sink and it will be dropped and hence packet modifier can be identified as packet dropper .To enable en-route detection of modifications, the afore-described procedures for packet sending and forwarding can be slightly modified as follows. When a node *u* has a data item *D* to report , it can obtain endorsement message authentication codes (MACs) from its neighbors, which are denoted as *MAC(D)*, following existing en-route filtering schemes such as the statistical en-route filtering scheme (SEF) and the interleaved hop-by-hop authentication scheme.

5. Performance Evaluation

The effectiveness and efficiency of the proposed scheme are evaluated in the ns-2 simulator (version 2.30). The detailed performance metric, methodology as well as the attack models is discussed in the supplementary file, available in the online supplemental material. The simulation results are presented in the supplementary file, available in the online supplemental material. We first study the impact of various system parameters on the detection. When there is no collusion. We then evaluate our proposed scheme under node collusion attacks .To identify packet modifiers and droppers, it has been proposed to add nested MACs to address this problem in [11] and [12]. We compare our proposed scheme with the PNM scheme [11] regarding detection performance and communication overhead. Details are presented supplementary file, available in the online supplemental material.

As the proposed scheme outperforms the PNM scheme in terms of detection performance and communication overhead, we further measure the computational overhead of the packet sending and forwarding scheme on TelosB motes, which are widely used resource-constrained sensor motes.

V. CONCLUSION

In this paper propose a simple yet effective scheme to identify misbehaving forwarders that drop or modify packets. In this 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 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 that behaviors of sensor nodes can be observed in a large variety of scenarios. Finally, most of the bad nodes can be identified by our heuristic ranking algorithms with small false positive. Extensive analysis, simulations, and implementation have been conducted and demonstrated the effectiveness of the proposed scheme. Our algorithm can be employed to inspect any aspects of networking activities, with the multiple attributes evaluated simultaneously. The algorithm is pure localized, thus scales well to large sensor networks. In this we notice that the detection algorithm can be specialized by exploring the degree of the correlation existent along with different aspects of sensor networking behaviors.

REFERENCES

[1] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang and Wensheng Zhang, “Catching Packet Droppers and Modifiers in Wireless Sensor Networks” in IEEE Trans on Parallel Distributed Systems, vol. 36, no. 5, May 2012.

[2] Vijay Bhuse, Ajay Gupta, and Leszek Lilien, “DPDSN: Detection of packet-dropping Attacks for Wireless sensor Networks,” Proc. Fourth Trusted Internet Workshop, 2005.

[3] 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.

[4] 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

[5] I. Krontiris, T. Ginneetsos, and T. Dimitriou, “LIDeA: A Distributed Lightweigth Intrusion Detection Architecture for Sensor Networks,” 2008.

[6]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.

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

[8] Z. Yu and Y. Guan, “ A Dynamic route Scheme for Filtering False Data in Wireless Sensor Networks,” Proc. IEEE en-INFOCOM, 2006.

[9] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. ACM MobiCom, 2000.

[10] H. Chan and A. Perrig, “Security and privacy in sensor networks,” IEEE Computer, Digital Object Identifier vol. 36, no. 10, pp. 103-105, Oct-2003.

[11]F. Ye, H. Yang, and Z. Liu,—Catching Moles in Sensor Networks,‖ Proc. 27th Int’l Conf. Distributed Computing Systems (ICDCS ’07), 2007.

[12] X. Zhang, A. Jain, and A. Perrig, —Packet-Dropping Adversary Identification for Data Plane Security,‖ Proc. ACM CONEXT Conf,2008.

SHORT BIOGRAPHY

Mr. M. Suresh received the **MCA** (2005-2008) from Sri Venkateswara University, Tirupathi, in **2008.** He Currently pursing **M.Tech (CSE) in Dept of Computer Science and Engineering** in PBR VITS Engg College, kavali, Nellore**,** under JNTUA University, Anantapur**.**

Vemula.V. Sunil Kumar has received his B.Tech in Electrical Communication Engineering and M.Tech degree in Computer science from JNTU, Hyderabad in 2002 and 2008 respectively. He is dedicated to teaching field from the last 11 years and he has 1 year industrial experience in BEL at Hyderabad. He has guided 12 P.G Students and 25 U.G students. His research areas included CN- MANETs, Neural Networks, and Image processing, embedded systems. At present he is working as Associate professor in PBR Visvodaya Institute of Technology & Science, Kavali, Andhra Pradesh, India.