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

International Journal of Advanced Research in Computer and Communication Engineering
Vol.2, Issue 12, December 2013

Improving High Throughput through Exploration of attacks in the wireless sensor network through collaborative clustering mechanism

Anu S[1], Dr.Umarani R[2]

Department Of Computer Science, Periyar University College Of Arts & Science, Mettur Dam, Tamilnadu, India[1]

Department Of Computer Science, Sri Saradha College For Women, Salem, Tamilnadu, India[2]

Abstract: Wireless Sensor networks deal with the challenging problem like node replication, packet dropping and modification by an adversary to disrupt communication. Many schemes have been proposed to mitigate or tolerate such attacks, but very few can effectively and efficiently identify the intruders through witness finding strategy, velocity exceeding strategy. To address this problem, propose a simple yet effective scheme to explore the attacks in the dynamic environment through clustering technique, which can identify Misbehaving forwarders that classify or destroy the packets. The detected intruders are placed into our devised collaborative defence mechanism is been employed to identify explored details of the attack and adopts suitable defence scheme to drop the strength and effect of the attack through revocation process. Extensive analysis and simulations have been conducted to verify the system performance.

Keywords: Wireless Sensor Network, Packet Dropping, Mitigating, Exploitation Attacks.

I. INTRODUCTION

In a 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. After compromising one or multiple sensor nodes, an adversary may launch various attacks [1] 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. To deal with packet droppers, a widely adopted countermeasure 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 of these paths can be tolerated. To deal with packet modifiers, most of existing countermeasures [6], [7], [8], [9] aim to filter modified messages 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, propose a simple yet effective scheme to catch both packet droppers and modifiers. In this scheme, a routing tree rooted at the sink is first established. When 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 marks, to the packet. This way, most of the bad nodes can be gradually identified with small false positive. Our proposed scheme has the following features: 1) being effective in identifying both packet droppers and modifiers, 2) low communication and energy overheads, and 3) being compatible with existing false packet filtering schemes; that is, it can be deployed together with the false packet filtering schemes, and therefore it cannot only identify intruders but also filter modified packets immediately after the modification is detected. Extensive simulation on ns-2 simulator has been conducted to verify the effectiveness and efficiency of the proposed scheme in various scenarios. In the rest of the paper, Section 2 defines the system model. Section 3 describes the proposed scheme and Section 4 reports the evaluation results. Section 5 discusses the related work, and Section 6 concludes the paper.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol.2, Issue 12, December 2013

II. NETWORK MODEL

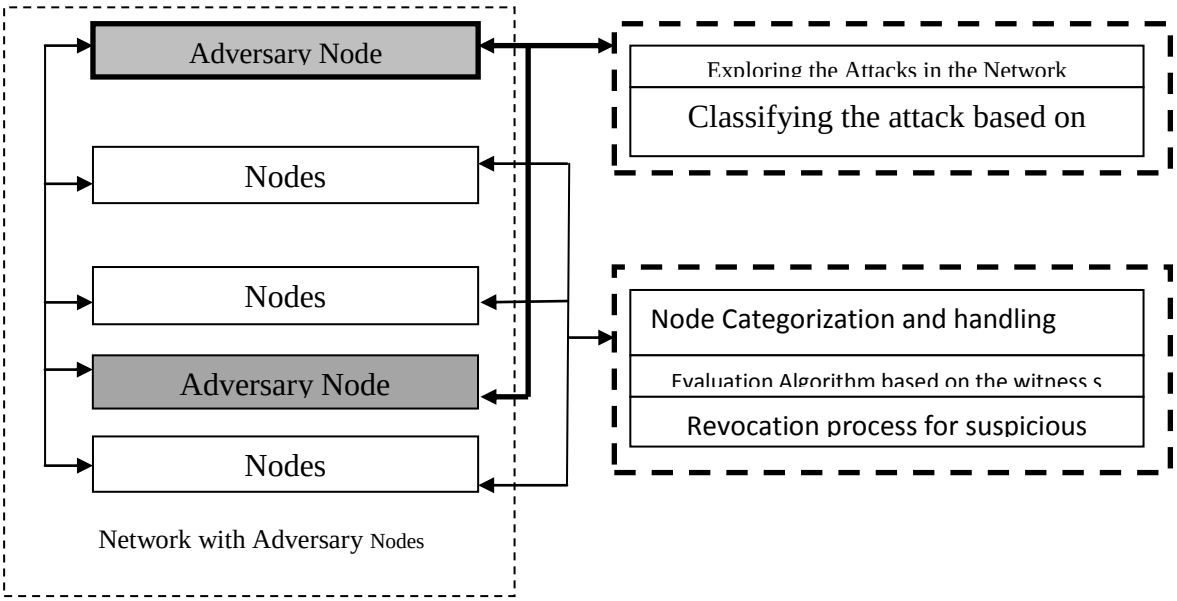

Fig 1 .Architecture diagram

Thus 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 aware of the network topology, which can be achieved by requiring nodes to report their neighbouring nodes right after deployment.

III. SECURITY ASSUMPTIONS AND ATTACK SCHEMES

Assume 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 the following two attacks:

Packet dropping: A compromised node drops all or some of the packets that is supposed to forward. It may also drop the data generated by itself for some malicious purpose such as framing innocent nodes.

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

IV. THE PROPOSED SCHEME

EXPLORING THE NODE REPLICAS IN THE DYNAMIC ENVIRONMENT

The low-cost, off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. Such attacks may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighbourhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, propose two new algorithms based on emergent properties, i.e., properties that arise only through the collective action of multiple nodes.

V. COLLABORATIVE CLUSTERING MECHANISM

The most straightforward detection scheme requires each node to send a list of its neighbors and their claimed locations to the base station. The base station can then examine every neighbour list to look for replicated nodes as follows.

A.Node replication Clustering algorithms may be Classified as listed below

- Hierarchical Clustering
- Probabilistic Clustering

By introducing the model of the proposed cluster-based revocation scheme, which can quickly revoke attacker nodes upon receiving only one accusation from a neighbouring node. The scheme maintains two different lists, warning list and blacklist, in order to guard against malicious nodes from further framing other legitimate nodes. Moreover, by adopting the clustering architecture, the cluster head can address false accusation to revive the falsely revoked nodes.

VI. RELIABILITY-BASED NODE CLASSIFICATION

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol.2, Issue 12, December 2013

According to the behavior of nodes in the network, three types of nodes are classified according to their behaviors: legitimate, malicious, and attacker nodes. A legitimate node is deemed to secure communications with other nodes. It is able to correctly detect attacks from malicious attacker nodes and accuse them positively, and to revoke their node structure in order to guarantee network security. A malicious node does not execute protocols to identify misbehaviour, vote honestly, and revoke malicious attackers. Feature extraction:

The data cluster is composed of the Node information with five features through the help of mobile agent in each sample such as, y1, y2, y3, y4 and y5, are extracted by the equation as follows:

$$yk = \frac{c^k}{\max_{i=1}^{5}\left(c^i\right)}$$

Where k=1, 2. . . 5, ck – Absolute sample of the replica nodes.

(1)The absolute information is calculated for different samples given by,

$$Y6=\log 10\left(\max_{m=1}^{5} c^m\right)$$

Thus, attack features are extracted, gives a feature vector Y = [y1 y2 y3 y4 y5 y6] T for attack diagnosis by hierarchical clustering logic and gives the complete description about the classified attack types of transformer.

If it discovers one or more replicas, it can revoke the replicated nodes by flooding the network with an authenticated revocation message. While conceptually simple, this approach suffers from several drawbacks inherent in a centralized system. First, the base station becomes a single point of failure. Any compromise of the base station or the communication channel around the base station will render this protocol useless.

VII. EXPERIMENTAL RESULTS:

The random way-point mobility pattern is used to model node movements. Each node is assumed to move to a randomly selected location at different velocities from 1 to 10 m/s. The Probability R that the newly joining node sensing each other with Hello packets in every time interval.

Optimal Threshold K

In this simulation prove the optimum threshold value in comparison with the numerical result.Set 80 nodes in the network, which contains eight malicious nodes and eight attacker nodes. In particular, focus on the value of obtained by using the policy As shown in the simulation results demonstrate that they are close to the mathematically analysed results.

VIII. COMPARING THE EFFECTIVENESS OF CERTIFICATE REVOCATION

Since the threshold method is able to release nodes to evaluate the effectiveness of our scheme,

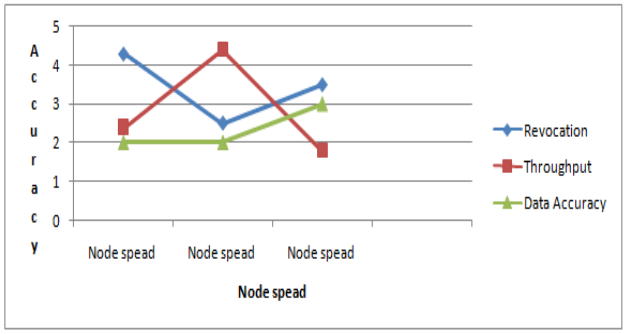

Fig 2.Comparing the Effectiveness of Certificate Revocation

First observe the change of the number of nodes in the WL according to different number of malicious nodes, and compare it with our previously proposed scheme. In this experiment, deploy 100 nodes in the network, where both the number of malicious and attacker nodes are set to 5, 10, 15, and 20 for each simulation run, respectively.

Fig. 2 clearly demonstrates that it can effectively reduce the number of nodes listed in the WL, i.e., the number of available nodes in the network has been improved by using the CCRVC scheme.See that the number of nodes listed in the WL is almost equal to the number of malicious nodes. To evaluate the impact of different numbers of attacker nodes on the revocation time, 50 legitimate nodes are considered in the network, while the number of attacker nodes is varied from 10 to 50. The revocation time changes with different numbers of attacker nodes between the existing schemes.

IX. ACCURACY OF RELEASING NODES

To study the accuracy of releasing nodes from the WL by using our proposed CCRVC scheme, first define the probability of the falsely released nodes and Run released means the probability of the unreleased legitimate nodes (legitimate nodes enlisted in the WL have not been correctly released).Examine the change of the accuracy in terms of different values of speed and density of the nodes.

X. CONCLUSION

Proposed and implemented a simple yet effective scheme to explore the attacks in the dynamic environment through clustering technique, which can identify Misbehaving forwarders that classify or destroy the packets. The detected intruders are placed into our devised collaborative defence mechanism is been employed to identify explored details of the attack and adopts suitable defence scheme to drop the strength and effect of the attack through revocation process. Extensive analysis and simulations have been conducted to verify the results.

REFERENCES

[1] H. Chan and A. Perrig, “Security and Privacy in Sensor Networks,” Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

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

[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, "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.