INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2919 - 2923
RECEIVED : 25.02.2018 PUBLISHED : 24.03.2018
March 24, 2018

DISTRIBUTED FINDING AND INHIBIT THE BYZANTINE ATTACKS IN WIRELESS SENSOR NETWORKS

[1]Mohanraj.K, M.Phil, Research Scholar, K.M.G College Of Arts & Science, Gudiyattam.

[2]Prof.P.Vinodhini, Asst. Professor, PG & Research Department Of Computer Science.

Abstract:

Wireless sensor networks tend to have a wide range of applications in our day to day life. In future, they can be used to survey our health, our home, the roads we follow, the office or the industry we work in or even the aircrafts we use, in an attempt to enhance our safety. But, these networks themselves are prone to security attacks. The list of security attacks is already very large and keeps on increasing with the expansion of these networks. A powerful tool for the detection of faulty or malicious nodes is the trust management schemes. Having detected the misbehaving nodes, their neighbours can use this information to avoid relying on them, either for data forwarding, data aggregation or any other cooperative function. There are a variety of trust models and most of them focus on defending against certain insider attacks. This paper discusses several security vulnerabilities that the trust mechanisms have. We also examine how inside attackers can exploit these security holes, and propose approaches that can mitigate the weaknesses of trust mechanisms.

Keywords: wireless sensor networks, security attacks, malicious nodes, insider attacks, trust mechanisms

1. INTRODUCTION

A vital security concern in wireless sensor network (WSN) is the insider threat. This is because inside attackers cannot be caught using traditional security mechanisms, like authentication an authorization, as they are the legal members of the network. These inside attackers can cause harm to the normal network functionalities by dropping, modifying or misrouting data packets. Thus, insider attacks are a serious threat for critical activities like military surveillance system and other critical infrastructures. Trust mechanisms have been developed with the notion of trust in human society. As the WSNs consist of hundreds or thousands of tiny sensor nodes, the trust mechanism is usually realized as a distributed system where each sensor is equipped with the capability to evaluate, update, and store the trustworthiness of other nodes based on the trust model. In general, working of trust mechanism consists of the following three stages 1) node behavior monitoring, 2) trust measurement, and 3) insider attack detection. A popular monitoring mechanism for the first stage is Watchdog [8]. A trust model such as beta trust model [4] and entropy trust model [10] processes the other two stages using the data collected by the watchdogs. These trust mechanisms work by continuously monitoring the behavior of the nodes and updating the trust value of the nodes. Each node has a watchdog which monitors the behavior of the neighboring nodes and lowers the trust value of the misbehaving neighbor. When the trust value of a certain node goes below a trust threshold, this node is termed untrustworthy and removed from the neighbor list. Though it seems to be a sound mechanism, but, there are several weaknesses in it. First, due to inherent weaknesses of WSNs, watchdog has some security vulnerabilities such as distributed sensors, limited transceiver range, and multi-hop

routing [5, 8]. Second, inside attackers cannot be prevented completely from dropping packets by any trust model. This is because packet can be dropped not only by an attacker but also due to contention or noise. Thus, an inside attacker can disguise its malicious behavior taking advantage of network traffic or noise. Third, we cannot ignore the fact that as insiders have internal knowledge about our network and security mechanisms against attacks, they can launch their attacks intelligently by exploiting such knowledge and avoid being detected. Many existing trust models with watchdog as their monitoring mechanism do not explicitly address these weaknesses. Our goal in this paper is to demonstrate how these insider attacks can pose threats to WSNs even after having a trust mechanism and watchdog, and to introduce defending approaches to improve the trust mechanism.

2. RELATED WORK

To safeguard our network, our WSN is assumed to be equipped with cryptography-based authentication and authorization to withstand outside attackers launching eavesdropping or packet modification [5]. In this WSN, outside attacks may be limited to directly damaging sensors by physical strike or jamming. Meanwhile, inside attackers have some advantages compared with outside attackers. First, as inside attackers can avoid our authentication and authorization, they can secretly cause damage to our network and it is difficult to foresee their attack patterns. Second, inside attackers can cause damage to the sensors and also disturb our network by dropping critical packets or by maliciously modifying packet information. Inside attackers can launch various types of active (modification, packet drop, or misrouting) as well as passive (eavesdropping) attacks. While modification, misrouting, and eavesdropping can be prevented to some extent by the authentication and authorization, it is quirky to counter packet drop attacks because for a particular packet drop, it is difficult to conclude that it is the result of an act by attacker or it is due to a collision or noise.

Moreover, inside attackers situated at a critical place in the network (e.g., near BS) can significantly deteriorate network performance such as packet delivery rate as a result of their repeated packet drops. There are several types of packet drop attacks such as Compared to blackhole attack, it is difficult to detect grayhole attack and on-off attack because of their complex attack patterns. Moreover, packet drop attacks have evolved to drop packets intelligently by exploiting inside knowledge about our network and security mechanism to avoid being detected. Each sensor node is required to monitor and record its neighbors' behaviors such as packet forwarding. In the next stage, this collected data will be used for evaluating trustworthiness. A popular monitoring mechanism used in this stage is watchdog. The confidence of the trustworthiness evaluation depends on the amount of data collected by a sensor and reliability of the collected data. This stage classifies a node to be either trustful or distrustful. The single most important parameter for this classification is the value of trust threshold (θT). This threshold must be chosen carefully as a low θT will misclassify attackers as trustful nodes and a high θT will cause unnecessary false alarm. However, if an attacker gets a reasonably good estimation on the value of θT, insider attacks can be launched without being detected. As shown below in Table 2, if the attacker assumes $\theta T = 0.7$, after certain number of initial successful forwarding (to build a high trust value), the attacker can drop a considerable number of packets consecutively without bringing its trustworthiness to 0.7 or below. For example, with s = 1000 previous successful forwarding, the next 428 packets can be dropped without being detected by the beta trust model, and 170 packets can be dropped if the entropy model is used.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2919 - 2923
RECEIVED : 25.02.2018 PUBLISHED : 24.03.2018
March 24, 2018

3. PROPOSED SYSTEM

In the previous sections, we have shown that even a single security vulnerability in trust mechanism can result in a huge damage on our network. Therefore, there is a need to eliminate the identified vulnerabilities and have countermeasures that provide a shield against inside attackers exploiting the security holes. In this section, we present approaches to defend against the security vulnerabilities in each step and some existing works with their advantages and disadvantages. As a consequence of limited overhearing distance, a sender S cannot completely monitor misbehaviors of a receiver or multiple colluding attackers. This limitation can be improved upon by increasing S's monitoring coverage with the help of other neighbors who can also contribute in monitoring all forwarding participants' behaviors in a routing path. This approach can reduce several types of colluding attacks. For example, two colluding attackers M1 and M2 located in a routing path S→M1→M2→BS, M2 can drop all packets without being detected by S due to the S's limited overhearing distance. On the other hand, in this approach. However, there are some limitations in these approaches. First, they do not address how their approaches can counter M2's selective packet drops against S. If M2 stores enough packets received from multiple nodes in its forwarding buffer, M2 can safely pinpoint S's packets by using a simple scheduling method so as not to trigger neighbor nodes' alert mechanism.

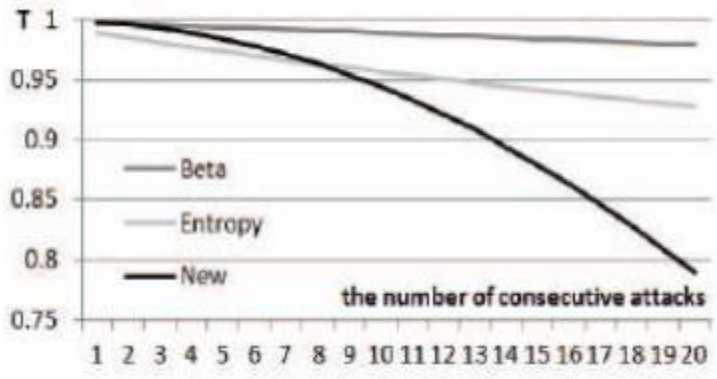

Fig.1.

To defend against M2's selective forwarding attack, neighbor nodes must be able to figure out which source node is under selective forwarding attack. These randomly chosen nodes will use the same but reversed routing path when they receive a packet. In case a previous checkpoint does not receive ACK from a next checkpoint, it reports an alert ACK to S or BS hop by hop along the same path. Then, S figures out which nodes are malicious or suspicious based on collected ACKs from checkpoints, and then discards them. This approach, however, has some weaknesses. First, while an ACK traverses back to S, inside attackers in the routing path can drop it as they dropped packets. Second, it is unclear how to accurately locate inside attackers. Third, it fails to handle when this checkpoints nodes falsely prosecute good nodes.

4. ANALYSIS

If an inside attacker figures out the working of trust evaluation function, it becomes easy for the attacker to estimate its trust values at its neighbors based on its packet drop attack rate. Once the attacker

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2919 - 2923
RECEIVED : 25.02.2018 PUBLISHED : 24.03.2018
March 24, 2018

knows its estimated trust values at others, it can intelligently adjust its attack rate never to be detected by its neighbors. Therefore, all critical functions (including source codes) must be hidden appropriately from even the owner (sensor). In fact, a sensor node may not need to know the trust evaluation function or exact trust values to do certain trust-related operations. For example, for trust-based packet forwarding, a sender only needs to pick up a trustful next hop to send its packet to BS via the next hop. A sender does not need to know the exact trust value of the next hop or how the next hop is chosen. That is, an authorized node should be allowed to access only necessary information. This can be achieved by using cryptography, authentication, and authorization. A trust threshold can be designed in static manner or dynamic manner. Static trust threshold might be optimal only for limited cases that we consider in the simulation. As a result, it may not be good for unconsidered situations. Meanwhile, dynamic trust threshold that adaptively changes according to situations in our network may have reasonably good results, although it may not be optimal for all situations. However, since dynamic trust threshold will be frequently computed, it must be designed in an energy-efficient way. It is apparent that the more redundancies we have, the more reliable our network is. However, we must keep in mind the redundancies are the cost we must pay. For example, in n multipath routing, a sending node first determines n disjoint multiple paths from itself to BS and then sends n identical packets along the n disjoint paths. Consequently, this may introduce at least n times of computation complexity and power that a single path routing requires. It is possible for him to find out sensitive information like as cryptographic keys or other important information when an attacker gets physical access to a sensor node. Self-devastation or tamper- proofing package is one solution of this [4]. In this process, when an outsider touches a sensor node physically, the node itself removes all its data or information and saves its own from the attacker. Whenever someone unauthorized or unconstitutional tries to access the node, it vaporizes the evidence and turn into empty.

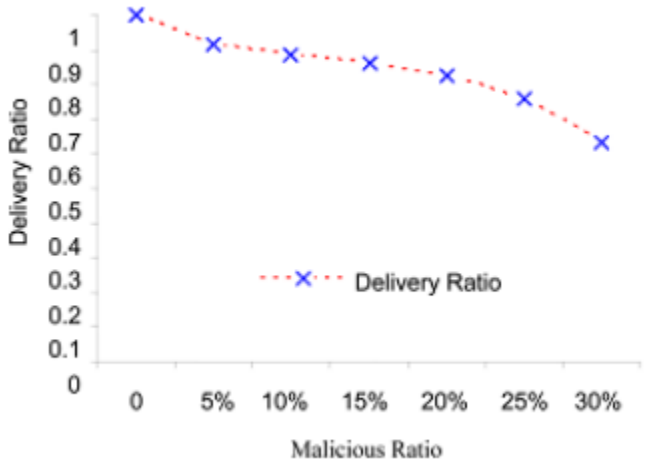

Fig.2.Output

An adversary passageway messages received in one part of the network over a low latency construction and replays them in a different part of the network in this attack. An adversary completely disrupts routing who is closely situated with the base station by creating a well-placed wormhole. Some nodes that are generally are multiple hops distant from a base station influenced by the adversary who are only one or two hopes away from them. They also find an easy way to transmit messages to the base station. Because of

short distance and high quality the new route is attractive to the legitimate nodes. This problem can overcome by making the original topographical route shortest from nodes.

CONCLUSION

In this attack an intruder sends HELLO packets to neighboring nodes informing them the survival of its own so that it can obtain and send them information packets. Laptop-class adversaries interconnect with such kind of packet to nodes in a particular area and make them believe that a genuine node is accessing with them. A large number of nodes within the network thus start sending packets to this invented node and mistreated. Proper authentication is the solution to this types attack. Due to the efficient activities in particular areas where regular wireless network is not capable of handling the communication, wireless sensor network efficiently maintain the communication between different users as well as with the nearest base station. The security threatening issue is one of the major drawbacks of this communication system. Malicious or bad intruders are present everywhere and they will remain for ever to gain success of their own by making this types of useful and important network defenseless or imperceptible. Engineers and researchers are also working hard to keep the system trustworthy and highly secured for outsiders.

REFERENCES

[1] Vladimir Dolzhenko, Sergey Klimenko and Alex Leonov; Meshnetics; Industrial Ethernet Book Issue, pp: 38-40, October 2005.http://www.iebmedia.com/index.php?id=5429&parentid=63&themeid=255&showdetail=true

[2] Waltenegus Dargie and Christian Poellabauer, Fundamentals of Wireless Sensor Networks, Wiley Series on Wireless Communicaions and Mobile Computing. pp. 268, ©2010.

[3] E. Shi and A. Perrig, “Designing Secure Sensor Networks,” Wireless Commun. Mag., vol. 11, no. 6, pp. 38–43, Dec. 2004.

[4] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, “A Survey Of Security Issues In Wireless Sensor Networks” , IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006.

[5] Tanveer Zia and Albert Zomaya, “Security Issues in Wireless Sensor Networks”, IEEE.

[6] Yee Wei Law, “Key Management And Link-Layer Security Of Wireless Sensor Networks”, Ctit Ph.D.-Thesis Series, Series Number: 1381- 3617, Ctit Number: 05-75, 2005.

[7] Raymond D.R. Midkiff.S.F, “Denial of Service in Wireless Sensor Network: Attacks and Defenses”, IEEE Pervasive Computing, Vol:7, Issue 1, PP: 74 – 81, March 2008.

[8] Mohit Saxena, “Security In Wireless Sensor Networks - A Layer Based Classification”, Cerias Tech Report 2007-04.