International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 1, May 2014, PP 65-69
www.arcjournals.org

In Mobile Sensor Networks Localized Algorithms for Detection of Node Replication Attacks

Sinthiya
M.E (CSE) I Year,
RVS College of Engineering and Technology,
Dindigul

S. Abirami
Assistant Professor Dept of CSE,
RVS School Of Engineering,
Dindigul

Abstract: *A wireless Sensor Network transfers the data one node to another node, energy efficient manner. The captured node, and place these replicas back into strategic positions in the network for further malicious activities. This is a so called node replication attack. The Range Based Detection Method (RBDM) to replication attacks are proposed to resist node replication attacks in mobile sensor networks. Finally, it can be network-wide revocation avoidance, time conception also avoided. The challenging problem of node replication detection. Although defending against node replication attacks demands immediate attention, compared to the extensive exploration on the defense against node replication attacks in static networks, only a few solutions in mobile networks have been presented. Moreover, while most of the existing schemes in Static networks rely on the witness-finding strategy, which cannot be applied to mobile networks, the velocity-exceeding strategy used in existing schemes in mobile networks incurs efficiency and security problems. Therefore, based on our devised challenge- and-response and encounter-number approaches, localized algorithms are proposed to resist node replication attacks in mobile sensor networks. The advantages of our proposed algorithms include localized detection; efficiency and effectiveness; network-wide synchronization avoidance; and network-wide revocation avoidance. Performance comparisons with known methods are provided to demonstrate the efficiency of our proposed algorithms. Prototype implementation on TelosB mote demonstrates the practicality of our proposed methods.*

1. INTRODUCTION

Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound pressure etc and cooperatively pass their data through the network to a main location. The ease of deploying sensor networks contributes to their appeal. They can quickly scale to larger configurations, since administrators can simply drop new sensors into the desired locations in the existing network. To join the network, new nodes require neither administrative intervention nor interaction with a base station; instead they typically initiate simple neighbor discovery protocols by broadcasting their restored credentials (e.g. their unique ID and/or the unique ID of their keys).

Unfortunately, sensor nodes typically employ low cost commodity hardware components unprotected by the type of physical shielding that could prevent access to a sensor's memory, processing, sensing and communication components. Cost considerations make it impractical to use the shielding that could detect pressure, voltage, and temperature changes that an adversary might use to access a sensor's internal state. Deploying unshielded sensor nodes in hostile environments enables an adversary to capture, replicate, and insert duplicated nodes at chosen network locations with little effort. Thus, if the adversary compromises even a single node can replicate it indefinitely, spreading the influence throughout the network. If left undetected, node replication leaves any network vulnerable to a large class of insidious attacks. Using replicated nodes, the adversary can subvert data aggregation protocols by injecting false data or suppressing legitimate data.

Previous approaches for detecting node replication typically rely on centralized monitoring, since voting systems cannot detect distributed replication. Centralized schemes require all of the nodes in the network to transfer a list of their neighbor claimed locations to a central base station that can examine the lists for conflicting location claims. If the adversary can compromise the base-station or interfere with its communications, then the centralized approach will fail. Also, the

nodes surrounding the base station are subject to an undue communication burden that may shorten the network's life expectancy.

In this paper, an optimized localization algorithm is introduced to detect the node replication attacks occurred in WSNs. The technique developed in these algorithms has the following advantages: Confined detection algorithms are beneficial to refuse node duplication attacks, provides better veracity, cancellation recession of the replicas that can be implemented by each node, instance management recession.

The rest of the paper is organized as follows. Section II presents a description about the previous research which is relevant to the flooding attacks and the possible solutions. Section III involves the detailed description about the proposed method. Section IV presents the performance analysis. This paper concludes in Section V.

2. REQUIREMENTS AND DESIGN FACTORS IN WIRELESS SENSOR NETWORK

Following are some of the basic requirements and design factors of wireless sensor network which serve as guidelines for development of protocols and algorithms for WSN communication architecture.

2.1 Fault Tolerance, Adaptability and Reliability

Sensor networks are required to operate through adapting to the environmental changes that sensors monitor. The networks should be self-learning. Reliability is the ability to maintain the sensor network functionalities without any interruption due to sensor node failure. Sensor node may fail due to lack of energy, physical damage, communications problem, inactivity, or environmental interference. The network should be able to detect failure of a node and organize itself, reconfigure and recover from node failures without losing any information.

2.2 Power Consumption And Power Management

One of the components of sensor nodes is the power source which can be a battery. The wireless sensor node being a microelectronic device, can only be equipped with a limited power source [04]. Over the remote inaccessible place with less human control and existence, power sources play critical role in survival of sensor nodes. Power source should be intelligently divided over sensing, computation, and communications phases as per requirement. Sensors can be hibernated when inactive. Lots of current researches are focusing on designing power-aware protocols and algorithms for wireless sensor networks. Recently, solar energy is also considered as an option for empowering remote sensor nodes which are exposed environment.

2.3 Network Efficiency and Data Aggregation

Flooding raw sensed data over the network can easily congest the network. Some critical applications like intruder detectors require urgent transmission and faster processing of data which may degrade performance and loose reliability due to congestion or latency in the network. Intelligent aggregation of sensed data and elimination of unwanted and redundant information and data compression can be a solution for efficient resource and energy utilization and congestion avoidance. Many algorithms like directed diffusion are proposed to facilitate data aggregation and dissemination within the context of WSNs.

2.4 Intelligent Routing: In Many Applications

Sensor nodes are moving nodes and can change place dynamically. Routing protocols must be adaptive to these changes and should be self-healing and self-configuring. The information should be persistent in spite of changes in network nodes. Low processing capacity of a node creates many challenges for routing packets throughout the neighboring nodes intelligently. As discussed above, some applications may require a faster communication and instant response. Routing algorithms should be intelligent to choose minimum hop and minimum distance paths for data transfer.

2.5 Management Challenge

Managing the communication over heterogeneous networks is basic challenge in self-managed system because policies and communication protocols plan an important role in network

communication. Also, it is necessary to balance the level of detail the network is providing to the client against the rate at which energy is being consumed while gathering the data. Clearly, it is preferable to have the network automatically do this tuning, rather than requiring manual intervention.

These basic requirements and design goals serve as challenge for current technology. Though current IP routing protocol exist and have significant applications in current networks and Internet, they do not satisfy complete design requirements in Wireless sensor networks because WSN nodes typically has limited computing capacities and less power. So WSN's require a different infrastructure and protocol stack which can be implemented using autonomic computing concept as we will discuss in next section.

3. RANGE BASED DETECTION METHOD (RBDM)

The Range-based Detection Method of the Replication Attacks

In this section, we propose to design a new distributed approach which does not require any nodes graphic position messages or system time synchronization for detecting node replication attacks in wireless sensor networks. The fundamental idea is to make use of the unique identification property: If a node has been detected, it could not appear in any other area. The RBDM is a range-based distributed detection method. In this paper, we use RSSI to estimate the distance between nodes. Each node estimates the distances between it and its neighbors by RSSI and executes the following two steps:

(Step 1) Categorizing neighbors:

We suppose that node a is a neighbor of node b(that is $x\ x\ R\ a\ b - \leq$). If $x\ x\ R / 2\ a\ b - \leq$, they are a pair of close neighbors, otherwise called far neighbors.

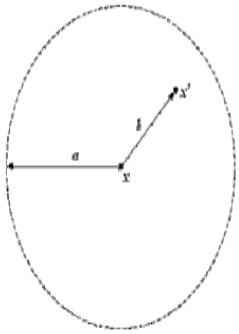
(Step 2) Constructing the detection information table of neighbors:

Each node records all identifications of its neighbors and set a flag signify their categorization. All of this information is stored in the neighbor-information table

Nodes in the network periodically broadcast own neighbor information table. By comparing nodes' neighbor-information table, we can detect replication attacks. In the following, we present three comparing criterion. When any of criterion in force, it means that replication attacks has been detected.

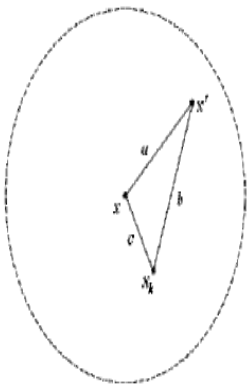
4. LUIC: LOCAL UNIQUE ID CRITERION

As shown in Fig. 1, if a replica x' has been deployed in the detection range of the compromised node x , they can detect each other (it means $x - x' \leq R$).



$a = R, b \leq R$

Fig. 1 LUIC: Local Unique ID Criterion



$R < a < \frac{3R}{2}, \frac{R}{2} \leq b \leq R, c \leq \frac{R}{2}$

Fig. 2 NUIC: Neighbor Unique ID Criterion

In this case, a same identification appears in the neighbor-information table of x , so that the LUIC come into force.

5. NUIC: NEIGHBOR UNIQUE ID CRITERION

Generally, replica node and compromised node cannot detect each other. Then the NUIC might be effective if we can find a node *k x* in network that can detect both replica *x′* and compromised node *x* , meanwhile *x′* and *x* are different neighbor of *k x* as In the neighbor-information table of *k x* , we can find *x′* and *x* with different flag. Then NUIC would divide into two symmetrical situations described as the following:

(Situation1)

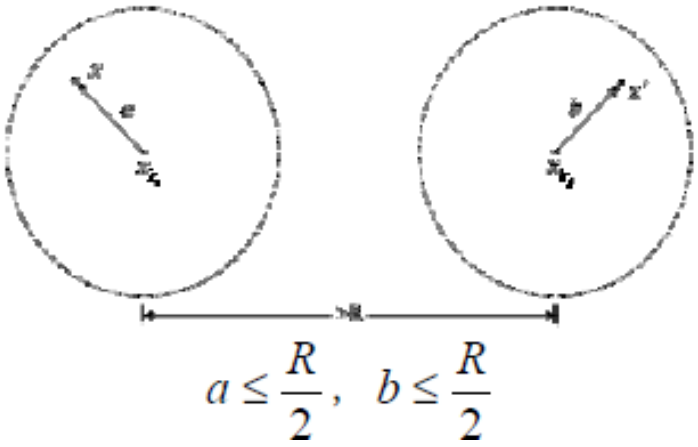
$$R<\left|x-x'\right|<\frac{3R}{2},\frac{R}{2}\le\left|x-x_k\right|\le R \text{ and} \left|x'-x_k\right|\le\frac{R}{2};$$

(Situation2)

$$R<\left|x-x'\right|<\frac{3R}{2},\frac{R}{2}\le\left|x'-x_k\right|\le R \text{ and} \left|x-x_k\right|\le\frac{R}{2};$$

6. GUIC: GLOBAL UNIQUE ID CRITERION

Obviously, the probability of LUIC or NUIC might be very low in a large region. In order to detect sparse distributed replicas, we should use neighbor-information tables of different nodes. *ki x* and *k j x* find a same identification (*x′* or *x*) as a close neighbor, however they cannot detect each other (it means *x x R ki k j* − >).



The same as *ki x* , *k j x* can find *x′* (or *x*) is record in its neighbor-information table with flag ‘00’ in such case. According to triangle theory, *ki x* and *k j x* might be neighbors, otherwise GUIC should be in force. The three criterions mentioned above are independent of each other, which can be test one by one in detection of

replication attacks. So we can calculate the total probability of detection by weighted accumulation of criterions. There are a number of routing protocols can be used to transmit neighbor-information tables of sensor nodes. In order to achieve comparisons of neighbor-information tables without store any received

Information, other complex criterions by analyzing more than two nodes’ neighbor-information tables will not be mentioned in this paper. In order to see whether these criterions can be implemented as a building block of an efficient distributed methods to detect node replication attacks, we analysis detection probability in the next section.

7. CONCLUSION

A range-based detection method (RBDM) has been supposed to detect replication attacks .simulation results demonstrated that the RBDM have excellent detection performance, and low communication/storage overhead, without system .synchronization time, correct node localization

or other additional information. Two replica detection algorithms for mobile sensor networks, XED and EDD, are proposed. Although XED is not resilient against collusive replicas, its detection

Frame work, *challenge-and-response*, is considered novel as Compared with the existing algorithms. Notably, with the novel Encounter-number detection approach, which is fundamentally? Different from those used in the existing algorithms, EDD not

Only achieves balance among storage, computation, and communication Overheads, which are all, but also possess unique characteristics, including network-wide time synchronization avoidance and network-wide revocation avoidance, in the detection of node replication attacks.

REFERENCES

[1] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst., Man, Cybern. C, Applicat. Rev., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[2] C. Bettstetter, H. Hartenstein, and X. P. Costa, "Stochastic properties of the random waypoint mobility model," Wireless Netw., vol. 10, no. 5, pp. 555–567, 2004.

[3] G. Cormode and S. Muthukrishnan, "An improved data stream summary the count-min sketch and its applications," J. Algorithms, vol.55, no. 1, pp. 56–75, 2005.

[4] M. Conti, R.Di Pietro, L. V. Mancini, andA.Mei, "Arandomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in Proc. ACMInt. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), Montreal, Canada, 2007, pp. 80–89.

[5] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans. Depend. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep./Oct. 2012.

[6] M. Conti, R. D. Pietro, and A. Spognardi, "Wireless sensor replica detection in mobile environment," in Proc. Int. Conf. Distributed Computing and Networking (ICDCN), Hong Kong, China, 2012, pp. 249–264.

[7] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in Proc. Int. ICST Conf. Security and Privacy in Communication Networks (Securecomm), Nice, France, 2007, pp. 341–350.

[8] R. Groenevelt, P. Nain, and G. Koole, "The message delay inmobile adhoc networks," Performance Evaluation, vol. 62, no. 1, pp. 210–228,2005.