Temporal Key Based Randomized Efficient and Distributed Detection of Clone Attack in WSNs

Wazir Zada Khan
E & E Engineering Department
Universiti Teknologi PETRONAS
Malaysia
wazirzadakhan@yahoo.com

Mohammed Y Aalsalem
School of Computer Science
Jazan University
Kingdom of Saudi Arabia
aalsalem.m@jazanu.edu.sa

Naufal M Saad
E & E Engineering Department
Universiti Teknologi PETRONAS
Malaysia
naufal_saad@petronas.com.my

Sultan Hamadi Aljahdali
College of Computer Science and Information System
Taif University
Kingdom of Saudi Arabia
aljahdali@tu.edu.sa

Abstract

Clone Node Attack is the most perilous threat to the security of wireless sensor networks. In this attack, an adversary compromises the captured node and replicates it, creating many replicas with the same node identity by obtaining all the secrets of the nodes. After this an adversary may launch many insidious attacks within the sensor network. Recent studies have shown that Randomized, Efficient and Distributed (RED) is considered to be the most promising distributed solution for detecting clone nodes but it also has some uncompromising shortcomings. In this paper we have presented a distributed, non-deterministic solution called Temporal Key Based RED (TKRED) which removes the drawbacks of RED by making enhancements in order to identify and revoke clones. Our simulation results have shown that proposed modification makes the protocol TKRED fully distributed and the witness node selection is non-deterministic.

Keywords; Node Replication Attack, Clones and Replicas, Wireless Sensor Networks, Clone Detection, Temporal Keys, Security.

1 Introduction

An adversary exploits the unattended nature of wireless sensor networks to physically capture and then compromises the sensor node. It then extracts the contents from the node and makes many clones of them which are also called replicas. By taking advantage of these replicas the adversary can launch many insider attacks as these node act as originals nodes.

In order to tackle with the node replication attack many detection techniques have been proposed. The proposed schemes are divided into two major classes Distributed and Centralized according to their nature of defense. In centralized techniques every node in the network sends its location claim to base station (sink node) through its neighboring nodes. Upon receiving the entire location claim at base station, the base station checks the node ids along their location, and if the base station finds two location claims with same id but different location, it raises a clone node alarm. On the other hand in distributed techniques the detection is performed by locally distributed node sending the location claim not to the base station (sink) but to a randomly selected node called witness node.

The centralized detection techniques mainly suffer from single node failure issue and the base station becomes the point of interest for adversaries as they try to target the base station. The nodes close to the sink also suffer from extra processing and quickly energy lost problems in sending and receiving all the traffic from the network to sink node. One kind of distributed techniques is called witness node based techniques which follow the claimer-reporter-witness framework. In witness node based techniques the claimer node locally broadcasts its location claim to its neighbors and each neighbor serves as a reporter node whose responsibility is to map the claimer id to one or more witness nodes. The major challenge for witness node based techniques is the selection and security of witness nodes. The selection of witness node must be non deterministic and should be randomly and uniformly distributed over the whole network so that the attacker will not come to know that which node is the witness node and ignores that node easily. These techniques also suffer from memory and processing over head as each node has to save some information for further processing.

Randomized, Efficient and Distributed (RED) protocol, proposed by Conti et al [4, 5] is considered to be the most promising witness node based solution developed so far for the detection of clones in wireless sensor networks. It is executed at fixed intervals of time and works in two steps. In the first step a random value, rand, is shared between all the nodes through some

978-1-880843-93-2 / copyright ISCA, CAINE 2013
September 25-27, 2013, Los Angeles, California, USA

central authority such as Base Station. The second step is called Detection phase in which each node broadcasts its claim (ID and location) to its neighboring nodes. Each neighbor node that hears a claim sends this claim with some probability to a set of pseudo-randomly selected network locations. The pseudo random function takes as an input: ID, random number, g. Every node in the path (from claiming node to the witness destination) forwards the message to its neighbor nearest to the destination. In each detection phase the replicated nodes will be detected by different witness nodes that are selected on the basis of random value distributed before every iteration of the algorithm by Base Station. Although RED has promising results, resolving the crowded center problem in [6], but besides that advantage, it has some severe drawbacks. The first major drawback of RED is that the selection of witness nodes is deterministic and depends upon random value rand which is shared between all the nodes through the Base Station. The distribution of random value is a big concern as no solution is provided in case if the base station is compromised. Secondly, it is also noted that the infrastructure for distributing RED's random seed may not always be available.

In this paper we seek ways to achieve efficient and robust clone node detection capability with lower communication, computation and storage costs than prior work. In order to meet this goal we have proposed a clone detection scheme which is a distributed and non deterministic solution by making enhancements in the RED protocol. Basically we have improved the first phase of RED by removing the involvement of base station for random value distribution. We have exploited the mechanism of temporal key integrity protocol (TKIP) [1] by modifying it to generate per-iteration seed for the pseudo-random function to select a random location. This innovatory and novel improvement will prevent cracking attempts and thwart an adversary to make clones or replicas. This is because even if an attacker obtains one security key i.e. time, he will not be able to use it for long as the system changes the security key used for data transmission every specified amount of time.

The rest of the paper is organized as follows: The section 2 describes the related work. Section 3 describes the network and adversary model. Section 4 presents TKRED protocol in detail. Section 5 presents simulation results for the assessment of area obliviousness of our protocol. Section 6 discusses some technical aspects regarding our proposed TKRED protocol. Finally Section 7 concludes the paper.

2 Related Work

To this point a number of schemes have been proposed for preventing and detecting node replication attacks in wireless senor networks. These schemes or techniques are broadly categorized into two types that are Centralized and Distributed techniques. A few of centralized techniques include [9, 10, 11, 12] and some of the distributed techniques include [3, 4, 5, 6, 8]. More details can be found in [14, 15, 16].

B.Parno et al. [6] have introduced two distributed algorithms for the detection of clone nodes in wireless sensor networks which are quite mature schemes as compared to DM. The first protocol is called Randomized Multicast (RM) which distributes location claims to a randomly selected set of witness nodes. The Birthday Paradox [7] predicts that a collision will occur with high probability if the adversary attempts to replicate a node. Their second protocol, Line-Selected Multicast (LSM), exploits the routing topology of the network to select witnesses for a node's location and utilizes geometric probability to detect replicated nodes. In RM, each node broadcasts a location claim to its one-hop neighbors. Then each neighbor selects randomly witness nodes within its communication range and forwards the location claim with a probability to the nodes closest to chosen locations by using geographic routing. At least one witness node is likely to receive conflicting location claims according to Birthday Paradox when replicated nodes exist in the network. In LSM the main objective is to reduce the communication costs and increase the probability of detection. Besides storing location claims in randomly selected witness nodes, the intermediate nodes for forwarding location claims can also be witness nodes. This seems like randomly drawing a line across the network and the intersection of two lines becomes the evidence node of receiving conflicting location claims.

Conti et al. have proposed a Randomized, Efficient, and Distributed protocol called RED [4, 5] for the detection of node replication attack. It is executed at fixed intervals of time and consists in two steps. In first step a random value, rand, is shared between all the nodes through Base station. The second step is called Detection phase. In the Detection phase each node broadcasts its claim (ID and location) to its neighboring nodes. Each neighbor node that hears a claim sends (with probability p) this claim to a set of pseudo-randomly selected network locations. The pseudo random function takes as an input: ID, random number, g. Every node in the path (from claiming node to the witness destination) forwards the message to its neighbor nearest to the destination. Hence the replicated nodes are detected by different witness nodes in each detection phase.

3 Network and Adversary Model

We have assumed that each node in the network is stationary and has a unique identifier (ID) which is assigned by the network operator before deployment. The sensor nodes are assumed to be not tamper resistant and an adversary has the capability of capturing and compromising a limited number of legitimate nodes in the network. After compromising a legitimate node, an adversary can replicate the compromised node. Moreover we have also assumed that an adversary cannot create new IDs for nodes but it has the ability to get full control of the compromised node and can produce many replicas of compromised nodes to enlarge the attack ability by deploying the clones back into the network. Finally we have assumed that all the

nodes know their geographic locations and are loosely time synchronized.

4 Enhanced Temporal Key based RED (TKRED)

In this section we propose an Enhanced Temporal Key Based Randomized, Efficient and Distributed (TKRED) protocol for the detection of node replication attack in wireless sensor networks. The idea of TKRED is inspired by the security mechanism of Temporal Key Integrity Protocol (TKIP) that wraps the WEP protocol in a sophisticated cryptographic and security techniques to overcome most of its weaknesses.

TKRED is an improvement of RED protocol in which random value is not broadcasted via a central authority (i.e. Base Station, Satellite etc) but a pseudo random function, running on all nodes of the network, will take the current time of the clock as its seed. This replacement will remove the major drawbacks of RED including the problem of unavailability of seed infrastructure. In TKRED, the witnesses are selected through a pseudorandom function which runs on all nodes of the network and it takes per-iteration seed from the modified TKIP (MTKIP) as shown in Figure 1. In MTKIP, per iteration seed is generated by following two phases. In the phase 1 the current time of the clock is concatenated (XOR) with the ID of the claimer node which results in an intermediate seed. This intermediate seed is then mixed with the sequence number of the iteration in phase 2 and results in a final per-iteration seed. Using this temporal based per-iteration input as a seed of a pseudorandom function will certainly decrease the communication and computation costs as there will be no need to distribute the seed among all the nodes. Also Base Station will not be required thus resolving the problem of single point of failure. TKRED is also more robust against node replication attacks as it employs even distribution of witnesses (i.e. it is also area-oblivious like RED which is also shown in Section V).

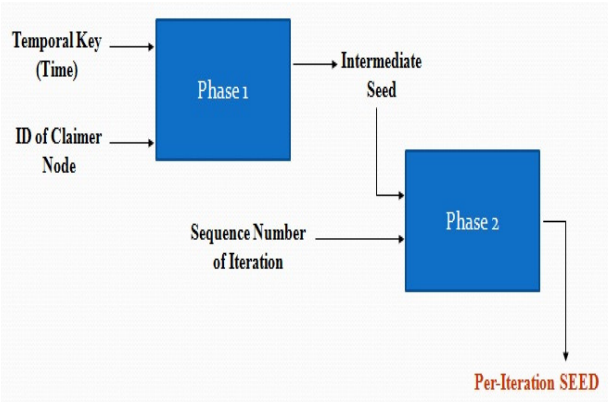

Figure 1: Modified TKIP (MTKIP) Based Seed Generation

Similar to RED, we have also assumed that the nodes in the network are stationary and loosely time synchronized and each node knows it geographic location by employing a GPS or other localization techniques. Our protocol executes when a new node joins the network (similar to [9]).

The working of TKRED is as follows. When a new node joins the network it will send its location claim to its neighbors which then forward the location claim with some probability to some randomly selected locations. These random locations are selected through a pseudo random function seeded by MTKIP. Then the location claim is forwarded to these randomly selected locations through GPRS routing protocol [2]. Nodes from the selected locations or closest to those locations will be selected as witness nodes. When these witness nodes find conflicting location claims, they will raise an alarm for detecting a clone node in the network and clone node will be revoked from the network.

5 Simulation and Results

In designing a protocol for the detection of clone attacks, a major issue lies in the selection and security of witnesses. An adversary is able to subvert the nodes and the attack goes undetected if an adversary gains the knowledge of future witnesses before the detection protocol executes. Here through simulation results it is justified that our proposed protocol TKRED is both ID and area oblivious and the security of witness nodes is guaranteed because TKRED neither provides any information about which ID of the sensors will be selected as the witness nodes nor it selects an area with high density of witnesses. In TKRED, the ID's of the witness are selected randomly among all the nodes and uniformly distributed throughout the network.

To assess area obliviousness of our protocol we study the witness distribution and simulate as follows. In our simulations we randomly deploy 1000 nodes within a 1000m x 1000m square. The transmission range is set to 50m. Figure 2 (a), 2(b), 2(c) and 2(d) shows that witnesses are selected uniformly and distributed from all over the network for different iteration of the protocol.

6 Discussion

The resistance of our protocol TKRED to a smart adversary lies in the fact that he cannot easily find out the witness nodes as time is used as an input of a pseudo random function by the reporter nodes to forward the location claim to randomly selected locations in the network. Using time as the seed of a pseudo random function guarantees that it is very hard for an adversary to locate or judge the witness node of any iteration. In the RED protocol, the set of witnesses for any node is fixed within each iteration and is known to anyone who has the knowledge of rand through either node compromise or sniffing the broadcast message containing the value of rand at the start of each iteration.

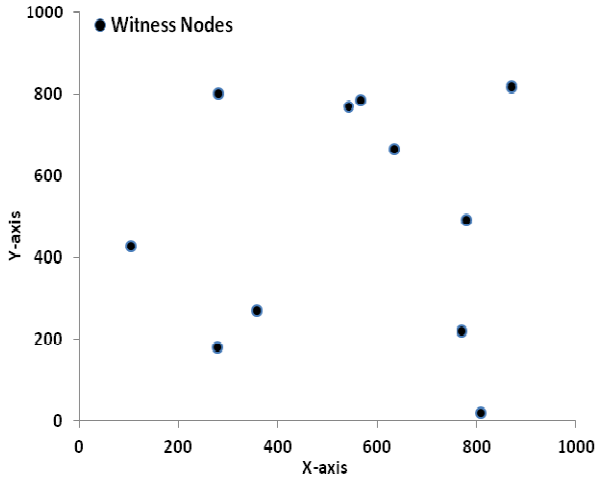

Figure 2(a): Protocol iterations showing Uniform Witness Distribution

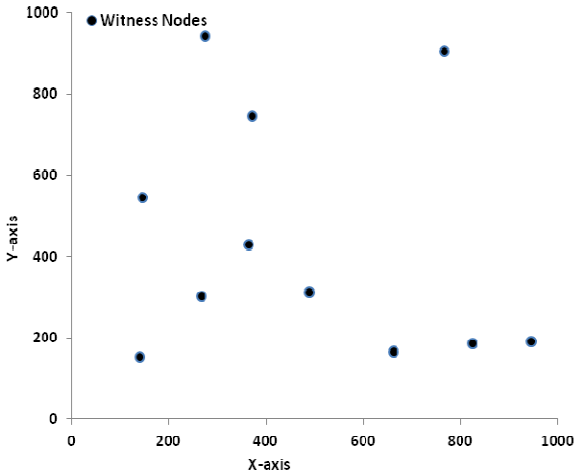

Figure 2(b): Protocol iterations showing Uniform Witness Distribution

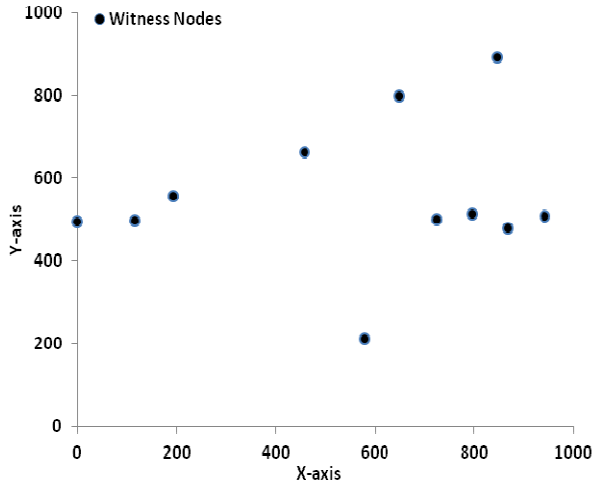

Figure 2(c): Protocol iterations showing Uniform Witness Distribution

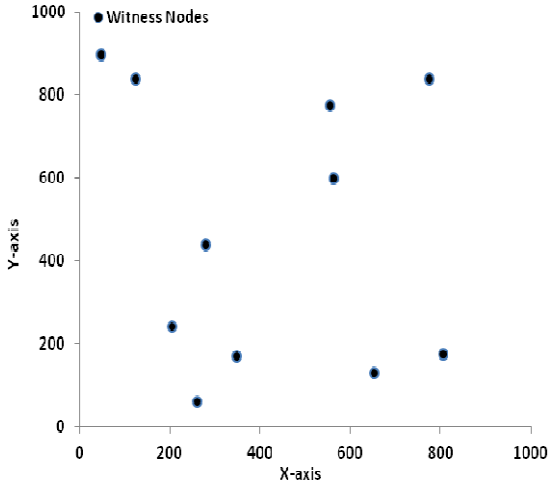

Figure 2(d): Protocol iterations showing Uniform Witness Distribution

But comparatively in our TKRED protocol it will probably be difficult for an adversary to compromise the witness node because the time is always changing and cannot be easily guessed. Also TKRED is executed whenever a new node is added into the network and the adversary is unable to judge that at which time the reporter node of this new node has sent its location claim. For better security purposes we can combine time with the ID of the claimer node as the seed of a pseudo random function. By using time which is continuously changing, the witnesses of a node are also changing in an unpredictable way and an adversary is unable to predict the appropriate time of every iteration whereas in RED, a very fast and smart adversary can easily acquire rand value.

7 Conclusion & Future Work

In this paper, we have proposed a protocol called TKRED as an enhancement to the existing RED protocol by exploiting the mechanism of TKIP for securing the network from clones and replicas. Through appropriate examples and intensive simulations its resiliency to a smart adversary is justified. Analyzing the security of TKRED, it is concluded that it is more robust, efficient and highly resilient against node replication attack and also ensures the security of witness nodes. The addition of time as the seed of a pseudo random function and elimination of the base station requirement will not only build greater security against clones but also the communication and computation overhead is also reduced noticeably.

In future, we will find out the solution for two types of attack scenarios. First in which a smart attacker compromises all the neighboring nodes of the network that in turn do not forward the location claim. In the second scenario the compromised nodes do not forward its location claim to its neighboring nodes.

Acknowledgment

The authors wish to acknowledge the anonymous reviewers for their valuable comments.

References

[1] Nancy Cam-Winget, Russ Housley, Davis Wagner, and Jesse Walker, Security flaws in 802.11 data link protocols " , Communications of the ACM Vol 46, Number 5, 2003 http://libaccess.sjsu.edu:2225/10.1145/770000/769823/p35-cam_winget.pdf.

[2] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," inProc. ACM MobiCom, 2000, pp. 243–254.

[3] J. W. Ho, D. Liu, Mathhew wright, Sajal K.Das ," Distributed Detection of Replica Node Attacks with Group Deployment Knowledge in Wireless Sensor Networks", Ad Hoc Networks, 2009, pp. 1476 – 1488.

[4] M. Conti, R. D. Pieto, and L. V. Mancini, "A Randomized Efficient and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks", In Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) , 2007.

[5] M. Conti, R. D. Pieto, L. V. Mancini and A. Mei. "Distributed Detection of Clone Attacks in Wireless Sensor Networks" in IEEE Trans, on Dependable and Secure Computing, 2011.

[6] B. Parno, A. Perrig and V. Gligor. "Distributed detection of node replication attacks in sensor networks", In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2005.

[7] A. J. Menezes, S. A. Vanstone and P. C. V. Orschot. "Handbook of Applied Cryptography", CRC Press, Inc., 1996.

[8] Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo, Li Xie, "Random Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks", IEEE Journal on selected areas in communications, Vol 28, june 2010.

[9] Zhu B, Setia S ,Jajodia S ,Roy S, Wang L. "Localized multicast: efficient and distributed replica detection in large-scale sensor networks" . IEEE Transactions on Mobile Computing 2010; 9(July) :913–26.

[10] 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 Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 37, no. 6, pp. 1246-1258, 2007.

[11] K. Xing, F. Liu, X. Cheng, D. H.C. Du, "Real-Time Detection of Clone Attacks in Wireless Sensor Networks", In Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS), pages: 3-10, 2008

[12] Heesook Choi, Sencun Zhu, and T. F. La Porta. "SET: Detecting node clones in Sensor Networks", In Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm), 2007.

[13] L. Eschenauer and V. D. Gligor, "A Key-management Scheme for Distributed Sensor Networks", in Proceedings of the 9th ACM conference on Computer and Communications Security, Washington, DC, USA, 2002, pp. 41-47.

[14] W. Z. Khan, M. Y. Aalsalem, N. M. Saad, and Y. Xiang, "Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 149023, 22 pages, 2013. doi:10.1155/2013/149023.

[15] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting Node Replication Attacks in Wireless Sensor Networks: A Survey," Journal of Network and Computer Applications, vol. 35, no. 3, pp.1022–1034, 2012.

[16] W. Z. Khan, N. M. Saad and M. Y. Aalsalem, " Scrutinizing Well-known Countermeasures against Clone Node Attack in Mobile Wireless Sensor Networks", International Journal of Grid and Utility Computing (IJGUC), Sep 2012.