

INTRUSION DETECTION AND PREVENTION OF NODE REPLICATION ATTACKS IN WIRELESS BODY AREA SENSOR NETWORK

Anandkumar K.M¹, Jayakumar C², Arun Kumar P³, Sushma M⁴ and Vikraman R⁵

Department of Computer Science and Engineering,
Easwari Enginerring College, Chennai

kmanandmss@gmail.com¹ cjayakumar2007@gmail.com² arunkumarp27@gmail.com³
sushma.m165@gmail.com⁴ rvikraman@hotmail.com⁵

ABSTRACT

Healthcare monitoring architecture coupled with wearable sensor systems for monitoring elderly or chronic patients in their residence has emerged as a promising technique. The wearable sensor system, built into a fabric belt, consists of various medical sensors that collect a timely set of physiological health indicators transmitted via low energy wireless communication (Zigbee) to mobile computing devices. In this context, Security of the Wireless Body Area Sensor Network (WBASN) in Ubiquitous healthcare applications is a crucial problem because sensitive and personal medical information must be protected against flaws and misdeed and also in order to increase user's acceptance to these new technologies. Moving towards this direction, we analyze the data access security due to replication attacks and the problems caused by it. We propose a secure multicast strategy that employs trust in order to evaluate the behavior of each node, so that only trustworthy nodes are allowed to participate in communications, while the replicated nodes are revoked from the network.

KEYWORDS

Wearable Sensor System, Wireless Body Area Sensor Network (WBASN), Wireless Sensor Network.

1. INTRODUCTION

Wireless Sensor networks have many useful applications and are expected to play an important role in various applications, e.g., assessing the “health” of machines; environmental, medical, food-safety, and habitat monitoring; energy management, inventory control, building automation, water management, precision agriculture etc. Therefore, such systems should at least guarantee the integrity and confidentiality of the information reported to the controlling authorities regarding the realization of environmental events. These are more or less standard security requirements that can also be found in traditional wired and wireless networks. However, the challenge is to satisfy these requirements under the special operating conditions of sensor networks. Towards this direction, we focus on the node replication attacks in Wireless Body Area Sensor Network (WBASN).

A Wireless Body Area Sensor Network (WBASN) is a collection of sensors with limited resources that collaborate to achieve a common goal. WBASNs can be deployed in human bodies where in the environments such as home and hospitals for measuring and monitoring the physiological parameters. The spread deployment of WBASNs during the last few years, introduces several security considerations. Sensors are resource-constrained tiny devices, with small memory storage capacities (10 KB of RAM and 48 KB of ROM), low computation

capacities (16-bit and 8 MHz CPU), and extremely limited energy supply (3.6 V), which is in general neither rechargeable nor replaceable. In addition, sensors are unshielded devices, work unattended, and are generally deployed in remote locations assimilated as hostile areas. All these facts yield WBASNs target to different attacks. For instance, an adversary could eavesdrop all network communications. Further, an adversary could capture nodes acquiring all the information stored, therein-sensors are commonly assumed to be not tamper-proof. Therefore, an adversary may replicate captured sensors and deploy them into the network to launch a variety of malicious activities. This attack is referred to as the clone attack or Replication attacks in WBASNs.

In replication attacks, attackers first compromises a node from the network, and then populate them into the network with replicas of it, using the secret key materials (node ID, secret cryptographic keys, etc.) which retrieves from the compromised node. Figure 1.1 shows the general system architecture of how an intruder enters the network. The aim of such attack is to have the control over the network, by compromising only few legitimate nodes. Since a clone has legitimate information, it may participate in the network operations in the same way as a non-compromised node and hence can launch a variety of attacks. For instance, a replica could create a black hole, initiate a wormhole attack with a collaborating adversary or inject false data or aggregate data in such a way to bias the final result, etc.

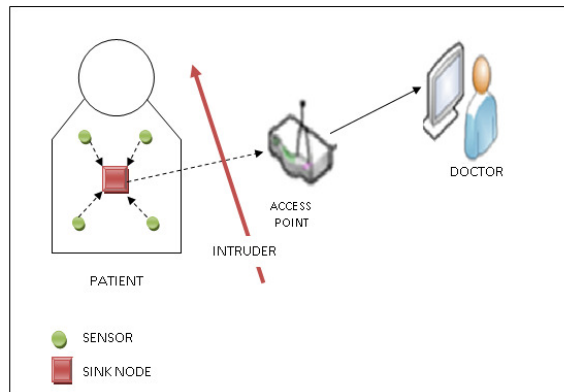


Figure 1: System Architecture of WBASN with Intrusion

To the best of our knowledge, most of the protocols proposed so far are only centralized or local protocols to cope with the replica attack. While centralized protocols have a single point of failure and high communication cost, local protocols do not detect replicated nodes that are distributed in different areas of the network. Therefore, we look for a network self-healing mechanism, where nodes autonomously identify the presence of clones and exclude them from any further network activity. In particular, this mechanism is designed to iterate as a “routine” event. It is designed for continuous iteration without significantly affecting the network performances, while achieving high clone detection rate.

We propose a new Secure Randomized Efficient and Distributed (SRED) protocol for the detection of node replication attacks and we prove that our protocol does meet all the requirements. Finally, extensive simulations of SRED shows that it is highly efficient as for communications, memory, and computations required and shows improved attack detection probability when compared to other distributed protocols.

The remainder of this paper is organized as follows: Next section reviews related work; Section 3 shows the threat model assumed in this paper; Section 4 describes the simulations that were carried out using our secure randomized efficient and distributed (SRED) protocol; Section 5

shows few experimental results on SRED and compares them with the results obtained in terms of detection probability, memory overhead, and energy overhead. These results confirm that SRED is more energy, memory, and computationally efficient, and detects node replication attacks with higher probability. Finally, Section 6 presents the concluding remarks.

2. RELATED WORKS

One of the first solutions for the detection of clone attacks relies on a centralized Base Station (BS) [2]. In this solution, each node sends a list of its neighbors and their locations (that is, the geographical coordinates of each node) to a BS. The same node ID in two lists with inconsistent locations will result in clone detection. Then, the BS revokes the clones. This solution has several drawbacks, such as the presence of a single point of failure (the BS) and high communication cost due to the large number of messages. Further, nodes close to the BS will have to be routing more messages than other nodes, hence shortening their operational life.

Another centralized clone detection protocol has been recently proposed in [3]. This solution assumes that a random key pre distribution security scheme is implemented in the sensor network. That is, each node is assigned a set of k symmetric keys, randomly selected from a larger pool of keys [4]. For the detection, each node constructs a counting Bloom filter from the keys it uses for communication. Then, each node sends its own filter to the BS. From all the reports, the BS counts the number of times each key is used in the network. The keys used too often (above a threshold) are considered cloned and a corresponding revocation procedure is raised.

Parno et al. proposed the work to address the node replication attacks [5]. They proposed two protocols: Randomized Multicast and Line-Selected Multicast. In Randomized Multicast, each node broadcasts a location claim to its neighbors. Then each neighbor selects some random locations within the network and forwards the location claim with a probability to the nodes closest to chosen locations by using geographic routing. According to Birthday Paradox [6], at least one node is likely to receive conflicting location claims when replicated nodes exist in the network. In order to reduce the communication costs and increase the probability of detection, they proposed Line-Selected Multicast protocol. 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 draw a line across the network, and the intersection of two lines becomes the evidence node of receiving conflicting location claims.

Zhu et al. proposed two more efficient distributed protocols for detecting node replication attacks: Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC) [7]. Both protocols need the sensor network to be a geographic grid, each unit of which is called a cell. In SDC each node's ID is uniquely mapped to one of the cells in the grid. When executing detection procedure, each node broadcasts a location claim to its neighbors. Then each neighbor forwards the location claim with a probability to a unique cell by executing a geographic hash function [8] with the input of node's ID. Once any node in the destination cell receives the location claim, it floods the location claim to the entire cell. Each node in the destination cell stores the location claim with a probability. Therefore, the clone nodes will be detected with a certain probability since the location claims of clone nodes will be forwarded to the same cell. The difference between SDC and P-MPC is the number of destination cells. In P-MPC the location claim is forwarded to multiple deterministic cells with various probabilities by executing a geographic hash function with the input of node's ID. The rest of procedure is similar to SDC. Therefore, the clone nodes will be detected with a certain probability as well.

Choi et al. proposed a clone detection approach in sensor networks called SET [9]. In SET the network is randomly divided into exclusive subsets. Each of subsets has a subset leader, and

members are one-hop away from their subset leader. Next, multiple roots are randomly decided to construct multiple sub-trees and each subset is a node of the sub-tree. Each subset leader collects member information and forwards to the root of the sub-tree. The intersection operation is performed on each root of the sub-tree to detect replicated nodes. If the intersection of all subsets of a sub-tree is empty, there are no clone nodes in this sub-tree. In the final stage, each root forwards its report to the BS. The BS detects the clone nodes by computing the intersection of any two received sub-trees. In summary, SET detects clone nodes by sending node's information to the BS from subset leader to the root node of a randomly constructed sub-tree and then to the BS.

Bekara and Laurent-Maknavicious proposed a new protocol for securing WSN against nodes replication attacks by limiting the order of deployment [10]. Their scheme requires sensors to be deployed progressively in successive generations. Each node belongs to a unique generation. In their scheme, only newly deployed nodes are able to establish pair-wise keys with their neighbors, and all nodes in the network know the number of highest deployed generation. Therefore, the clone nodes will fail to establish pair-wise keys with their neighbors since the clone nodes belong to an old deployed generation.

The only approach that achieves real-time detection of clone attacks in WSN was proposed by Xing et al. [11]. In their approach, each sensor computes a fingerprint by incorporating the neighborhood information through a superimposed s -disjunct code [12]. Each node stores the fingerprint of all neighbors. Whenever a node sends a message, the fingerprint should be included in the message and thus neighbors can verify the fingerprint. The messages sent by clone nodes deployed in other locations will be detected and dropped since the fingerprint does not belong to the same "community".

Conti et al. proposed a recent work for detection of node clone attacks in WSNs called RED based distributed detection [13]. When executing RED, the BS broadcasts a random value to all nodes in the network. Then the following operations are similar to Parno et al.'s scheme except for the selection of witness nodes. In RED the witness nodes are selected based on a pseudo random function with the inputs of node's ID, random value which is broadcasted by the BS and the number of destination locations. Location claims with the same node ID will be forwarded to the same witness nodes in each detection phase. Hence the replicated nodes will be detected in each detection phase. When next time the RED executes, the witness nodes will be different since the random value which is broadcasted by the BS is changed.

In this paper, we review the contribution of [1] and further thoroughly investigate the feasibility of the SRED protocol. The analysis and the further set of simulations presented show that the SRED protocol can be actually implemented in sensor network. Also, it can be continuously iterated over the same network, as a self-healing mechanism, without significantly affecting the network performance (nodes energy and memory) and the detection protocol itself.

3. THREAT MODEL

We consider a hospital scenario as shown in figure 3.1 where, there are four patients in an ICU. Each patient has a set of sensors on their body which forms a WBAN. These nodes send their information to a sink node which collects and then forwards it to the access point. The access point forwards the data to the doctor who should respond with the required prescription. Now this information is further forwarded to the local care giver (nurse) who is also placed in the ICU and can medicate the patient according to the doctor's prescription.

We define a simple yet powerful adversary. It can compromise a certain fixed amount of nodes and replicate one or more into multiple copies (the clones). In general, to cope with this threat, it could be possible to assume that nodes are tamper-proof. We also assume that the patients are stationary and also that there are no replicated BANs at the time of initialization. The adversary would be in and around the hospital environment so that he comes in the range of communication with the particular access point nearer to the ICU and launches a clone attack. He then, compromises a few nodes (one BAN), using the cryptographic information obtained from the compromised nodes to produce replicas and finally inserts the replicated BAN into the network. The compromised nodes and replicated BAN are fully controlled by the adversary and can communicate with each other at any time. In this manner he modifies the required data and sends it to the access point.



Figure 2: Threat Model

4. SIMULATION & RESULTS

The proposed model simulation was carried out using the crossbow kit and the readings were noted using the moteview software as shown in figure 4.1. The simulation was done over a time of 100ms. Initially six motes were used for communication to show the normal scenario and readings were noted. Later two nodes were replicated and the communications were carried on.



Figure 3: Arrangement of sensor motes with coordinator

Figure 3 shows the star topology arrangement of sensors with coordinator using the mote view

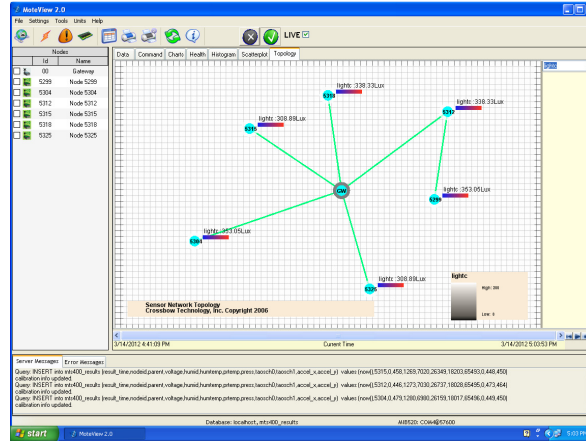


Figure 4: Topology arrangement of sensors without replication of motes ID

After the node replication is done, the original and the replicated sensors send its data alternatively to the access point. The original sensors will be directly sending data to the access point where as the replicated sensors sends its data to the access point only through multi-hops as shown in figure 4 and figure 5 respectively.

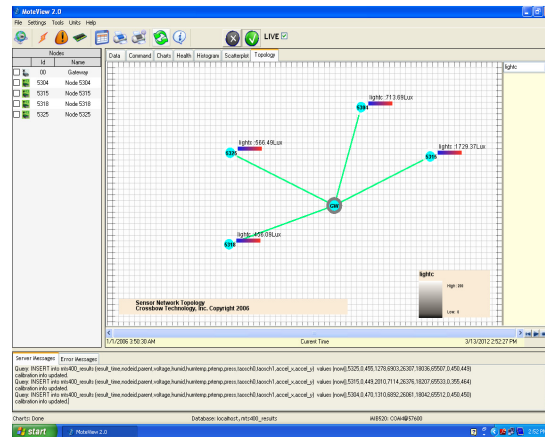


Figure 5: Topology of original sensors sending data

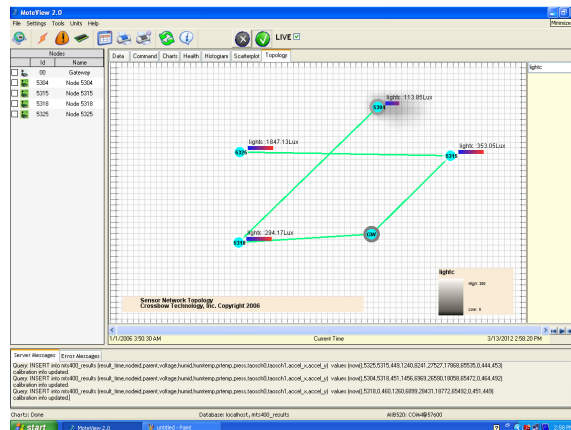


Figure 6: Topology of replicated sensors sending data through multi-hops.

Figure 7 shows a table of sample data after replication of two sensors. It was noted that the parameters (eg: Light & Temperature) keeps varying drastically during the simulation time. These variations of values are clearly shown in figure 8 & figure 9.

ID	Name	Voltage	Temperature	Humidity	Light	...
5304	Node 5304	2.66 V	41.44 °C	28.84 C	28.42 C	1000.65 mb
5315	Node 5315	2.66 V	40.79 °C	30.04 C	30.47 C	1001.45 mb
5318	Node 5318	2.70 V	41.46 °C	28.8 C	28.88 C	996.41 mb
5326	Node 5326	2.70 V	38.5 °C	30.45 C	30.24 C	1000.3 mb

Figure 7: Sample readings of sensors

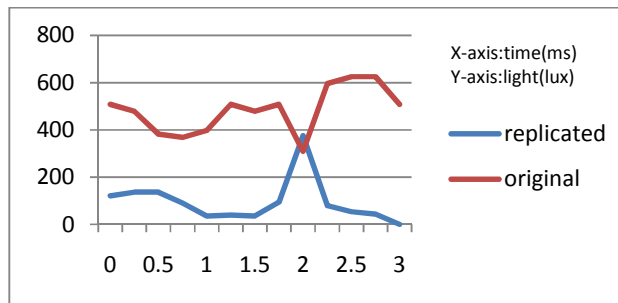


Figure 8: Comparison of graph for original and replicated node ID 5304 with varying parameter as a light.

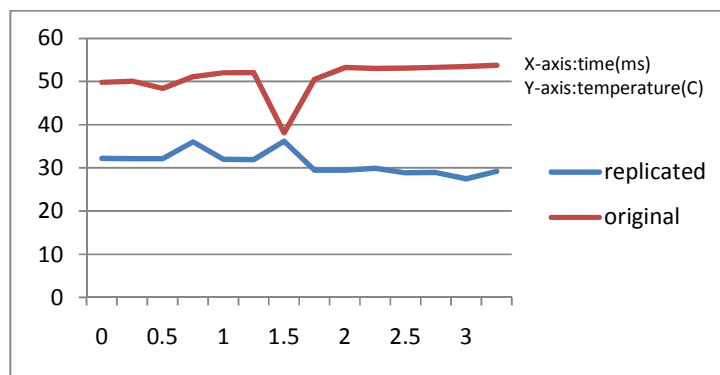


Figure 9: Comparison of graph for original and replicated node ID 5304 with varying parameter as a temperature

Figure 10 shows the topology in the mote view of the replicated sensors which are in a dark room or less intensity of light.

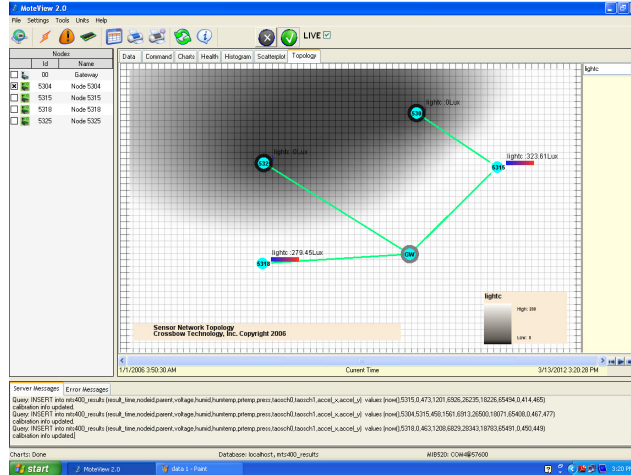


Figure 10: Intensity of light at the moment when one get replicated

The above snapshots and graphs shows that the required simulations were carried out and the results were noted.

5. COMPARISONS

Simulations were carried out using SECURE RED algorithm for parameters (Light and Temperature). Table 1 illustrates memory and communication costs for each protocol. Using this table, analysis was made to show how SECURE RED algorithm is efficient over the other existing protocols. Figure 11 shows the comparison results between RED and SRED. The constraints that were taken into considerations are

1. Detection rate
2. Energy constraint
3. Memory overhead

PROTOCOLS	COMMUNICATION	MEMORY
Broadcast	$O(n^2)$	$O(d)$
Line-Selected Multicast	$O(n\sqrt{n})$	$O(\sqrt{n})$
Randomized Multicast	$O(n^2)$	$O(\sqrt{n})$
Deterministic Multicast	$O(g\sqrt{n})$	$O(g)$
Randomized Efficient Distributed Multicast	$O(g.p.d.\sqrt{n})$	$O(g.p.d)$
Our Method(SRED)	$O(g.p.d.n)$	$O(\sqrt{n})$

Table 1: summary of protocol cost

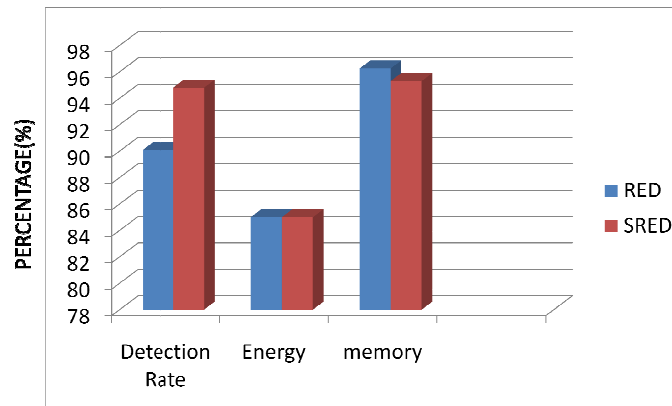
PERFORMANCE ANALYSIS

Figure: 11 Performance Measure

From the above graph it was interpreted that overall efficiency of RED algorithm was 90.45% and SECURE RED algorithm was 91.7%. Thus we conclude that SECURE RED algorithm is 1.25% more efficient than the RED algorithm.

6. CONCLUSION

In this paper, we presented and justified a few basic requirements for node replication attacks under pervasive health care environments. In particular, we have introduced new adversary threat models. However, a major contribution of this paper is the proposal of a self-healing, randomized, efficient, and distributed protocol to detect node replication attacks. We analytically compared RED with SRED and proved that the overhead introduced by RED is high and almost evenly unbalanced among the nodes. Extensive simulations confirm these results. Lastly, also in the presence of compromised nodes, we can analytically show that SRED is more resilient in its detection capabilities than RED.

REFERENCES

- [1] Mauro Conti, Luigi Vincenzo Mancini, and Alessandro Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks", IEEE Transactions on Dependable and Secure Computing., vol. 8, no. 5, September/October 2011
- [2] L.Eschenauer and V.D.Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Conf. Computer and Comm. Security (CCS '02), pp. 41-47, 2002.
- [3] R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "On the Detection of Clones in Sensor Networks Using Random Key Predistribution." IEEE Trans. Systems, Man and Cybernetics, Part C: Applications and Rev., vol. 37, no. 6, pp. 1246-1258, Nov. 2007.
- [4] C. Bekara, M. Laurent-Maknavicius. "A new protocol for securing wireless sensor networks against nodes replication attacks", In Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2007.
- [5] B. Parno, A. Perrig, and V.D. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symposium. Security and Privacy, pp. 49-63, May 2005.

- [6] A. J. Menezes, S. A. Vanstone and P. C. V. Orschof. "Handbook of applied cryptography", CRC Press, Inc., 1996.
- [7] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy. "Efficient distributed detection of node replication attacks in sensor networks", In Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC) , 2007.
- [8] S. Ratnasamy, B. Karp, L. Yin, F. Yu, D. Estrin, R. Govindan, and S. Shenker. "GHT: A geographic hash table for data-centric storage", In Proceedings of the 1st ACM International Conference on Wireless Sensor Networks and Applications (WSNA), 2002.
- [9] 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.
- [11] C. Bekara, M. Laurent-Maknavicius. "A new protocol for securing wireless sensor networks against nodes replication attacks", In Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2007.
- [12] 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), 2008.
- [13] K. Xing, X. Cheng, L. Ma, and Q. Liang. "Superimposed code based channel assignment in multi-radio multi-channel wireless mesh networks", In Proceedings of the 13th Annual International Conference on Mobile Computing and Networking (MobiCom), 2007.
- [14] Mauro Conti, Luigi Vincenzo Mancini, and Alessandro Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks", IEEE Transactions on Dependable and Secure Computing., vol. 8, no.5,September/October 2011