Journal of Computer Science 8 (10): 1691-1699, 2012
ISSN 1549-3636

Pro-Active Prevention of Clone Node Attacks in Wireless Sensor Networks

[1]Anandkumar, K.M. and [2]C. Jayakumar
[1]Department of Computer Science and Engineering,
Easwari Engineering College, Anna University, Chennai, India
[2]Department of Computer Science and Engineering,
R.M.K. Engineering College, Anna University, Chennai, India

Abstract: Problem statement: Wireless mobile sensor networks are deploying large, self-organized and adaptable sets of sensors for many applications such as military, environmental, health care, remote monitoring and other applications. Unfortunately, the simplicity and low-cost of these sensors make eases cloning of compromised nodes by attackers in the network. Due to the unattended nature of wireless sensor networks, an adversary can capture and compromise sensor nodes, make replicas of them and then mount a variety of attacks with these clones. This cloning attack is the entry point for a large span of creepy attacks. In such attack, an adversary uses the credentials of a compromised node to introduce the replicas secretly into the network. These replicas are then used to launch a variety of attacks that challenge the sensor applications. Therefore the detection of node replication or called clone attacks in a wireless sensor network is a fundamental problem. **Approach**: These clone node attacks are highly dangerous because they allow the attacker to compromise a few nodes to exert control over much of the network. Several clone node detection schemes have been proposed in the literature to defend against such attacks in static sensor networks. A few distributed solutions to address this fundamental problem have been recently proposed. However, these solutions are not satisfactory in *Pro-active* context. First, they are energy and memory demanding: A serious drawback for any protocol to be used in the WSN-resource-constrained environment. Further, they are vulnerable to the specific adversary models introduced in this study. To overcome the above problems we propose the improved version of Randomized, Efficient and Distributed protocol named SRED-Secure, Randomized and Efficient and Distributed protocol. We show that our emergent algorithms represent a promising new approach to sensor network security by improving its trust aspects with the witness node. **Results:** The result of the experiments shows that not only the improvement levels of security aspects but also shows that the considerable amount of improvements in memory and time overheads. **Conclusion:** This method improves the security aspect of wireless sensor networks mainly in unattended environment and improves the real time data acquisition systems in future era.

Key words: Clone detection, sensor networks, Wireless Body Area Sensor Network (WBASN), security, secure RED method

INTRODUCTION

A Wireless Sensor Network (WSN) is a distributed and ad hoc network constituted by a large number of tiny-size, low-cost and resource-constrained sensor nodes. Due to cost concerns, current generations of sensor nodes lack hardware protection for tamper-resistance, but are often deployed in unattended and harsh environments and thus are susceptible to capture and compromise. In potentially antagonistic environments, the security of unattended mobile nodes is extremely critical. The attacker may be able to capture and compromise sensor nodes and then use them to inject counterfeit data into the network, interrupt network operations and eavesdrop on network communications. In this scenario, a particularly dodgy attack is the clone node attack (Parno *et al*., 2005), in which the adversary takes the secret keying materials from a compromised node, generates a large number of attacker controlled replicas that share the compromised node’s keying materials and ID and then spreads these replicas throughout the network. With a single captured node, the adversary can possible to create as many replica nodes in the network.

Corresponding Author: Anandkumar, K.M., Department of Computer Science and Engineering, Easwari Engineering College, Anna University, Chennai, India Tel: +919442512377

MATERIALS AND METHODS

The time and effort needed to inject these replica nodes into the network should be much less than the effort to capture and compromise the equivalent number of original nodes. The replica nodes are controlled by the adversary, but have keying materials that allow them to seem like authorized participants in the network. Protocols for secure sensor network communication would allow replica nodes to create pair wise shared keys with other nodes and the base station, thereby enabling the nodes to encrypt, decrypt and authenticate all of their communications as if they were the original node. A straightforward solution to stop replica node attacks is to prevent the adversary from extracting secret key materials from sensor nodes by equipping them with tamper-resistant hardware (Ho *et al*., 2011).

There are many replica node detection schemes have been proposed for static sensor networks (Parno *et al*., 2005), (Conti *et al*., 2007), (Xing *et al*., 2008). The primary method used by these schemes is to have nodes report location claims as a finger print that identifies their positions and for other nodes to attempt to detect conflicting reports that single node in multiple locations.

In this study we propose an effective and Fig. 1 efficient *pro-active* method called Secure, Randomized and Efficient and Distributed protocol (SRED) to detect node replication attacks in wireless sensor networks. In the recent work published so far says about node replication attacks in static wireless sensor network by identifying the clone based on its location after the attack was happened. But our proposed method finds the clone before it was introduced into the network by the adversary and allows continuous communication between the nodes by avoiding the blocking state in between the nodes due to the clone attack. Our extensive simulations results also show that there is an improvement comparatively with previous methods and our algorithm effectively block the entry of any clone nodes into the network.

The rest of the study is organized as follows: Related works, Threat model for our scheme, Secure multicast mechanism and the proposed pro-active preemptive protocol called Secure, Randomized and Efficient and Distributed protocol (SRED) along with security and performance analysis, Results of simulations that we conducted to evaluate the proposed scheme, Comparison of our method (SRED) with the existing RED Scheme and Finally concludes the study.

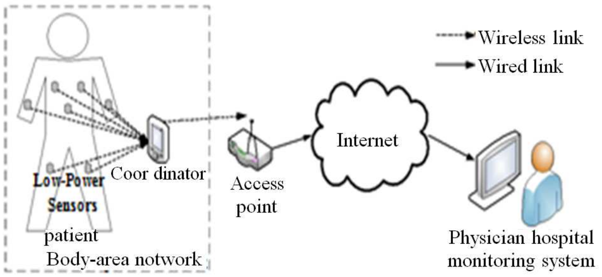


Fig. 1: Model scenario-the wireless patient monitoring system

Related works: One of the first solutions for the detection of clone attacks relies on a centralized Base Station (BS) (Eschenauer and Gligor 2002). 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 be required to route much more messages than other nodes, hence shortening their operational life.

Another centralized clone detection protocol has been recently proposed in (Brooks *et al*., 2007). 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 (Bekara and Laurent-Maknavicius, 2007). 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*. (2005) proposed the work to address the node replication attacks. 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 (refer to as witness nodes) closest to chosen locations by using geographic routing. According to Birthday Paradox (Menezes *et al*., 1996), at least one witness 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*. (2007) proposed two more efficient distributed protocols for detecting node replication attacks: Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC) (Zhu *et al*., 2007). 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 (Ratnasamy *et al*., 2002) 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*. (2007) proposed a clone detection approach in sensor networks called SET. 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 (Bekara and Laurent-Maknavicius, 2007). 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*. (2008). In their approach, each sensor computes a fingerprint by incorporating the neighborhood information through a superimposed *s*-disjunct code (Xing *et al*., 2007). 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*. (2007; 2011) proposed a recent work for detection of node clone attacks in WSNs called RED based distributed detection (Conti *et al*., 2011). 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*. (2005) 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.

Threat model: We now, consider a hospital scenario as shown in Fig. 2 where, there are four patients in an ICU. Each patient has a set of sensors on their body which forms a Wireless Body Area Sensor Network (WBASN). 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 would respond with the required prescription. Now this information is further forwarded to the care giver who is also placed in the ICU and can medicate the patient according to the doctor's prescription.

We now 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).

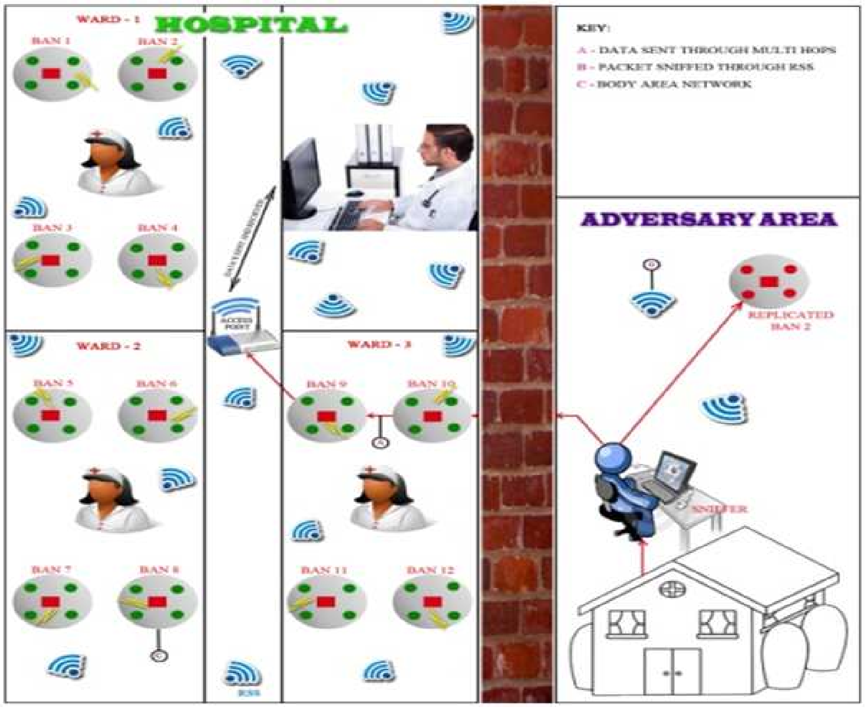


Fig. 2: Threat model

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 stationery and also that there are no replicated WBASNs 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 WBASN), using the cryptographic information obtained from the compromised nodes to produce replicas and finally inserts the replicated WBASN into the network. The compromised nodes and replicated WBASN 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.

Based on our practical experience, In WBASN the entry of clone nodes directly through the gateway or access pointer with same SSID is possible. But if the access pointer is more intelligent it can capable to block the communication or accepting the data from the original and clone nodes. Here we worked with layer 2 and layer 1 level with sensor motes. The access pointer accepts the data from the original and malicious nodes with different time intervals and also simultaneously it records the data on database. The recorded reading shows high variations between peak to peak and it makes confusion to the reader and causes the various hazards to the monitoring body. If the gateway is capable to block the same ID communication, it discards the conflict ID and data from the nodes and also announce to all the nodes about the replication event. Normally the adversary injects the malicious node through any one of the intermediate node via a multi hop communication and try to reach the gateway or access pointer. In this context the node accepting the new entry node does not know about their presence in the network, if it not properly updated or the updating time get too long, when the sensor network field is very large. In this case we present our algorithm and distribute randomly to the nodes available in the network which checks and prevent the new entry node based on few constraints and allowed or blocked for further communication. The removal of malicious node will happen ahead of the gateway and it can allow continuous communication with all other nodes. so it pro-actively prevents or blocks the malicious node by effectively blocking the malicious node in the entry point level itself.

RESULTS AND DISCUSSION

The pro-active prevention of malicious node into the network can be done by comparing its location information with gateway and all other nodes by updating the Message Information Table (MIS). The message information table consist deployment and node location information. The verifying node also selects some of the witness randomly in the network and compare with the gateway information. If both are match it concludes that the presence of malicious node or the other possibility.

PRO-active preemtive protocol:

Secure Multicast Mechanism: In the above Fig. 2 all the three wards consist of 12 WBASNs namely WBASN 1 to WBASN 12. Considered WBASN 2 gets replicated and try to intrude into the network. Whenever there is a chance the cloned or duplicated nodes try to enter through nearby accessible trusted WBASN. In our assumption consider the node 2 gets cloned. In the above scenario cloned node WBASN 2 enter through WBASN 10 available in the ward 3 and reach the access pointer/base station via intermediate node WBASN 9 and try to reach the access pointer and make a update in the information table available. Now the access pointer gets confused because of two similar WBASN 2 IDs (already the trusted / original WBASN 2 communicating from ward 1). After the attack happens in the access pointer it denies to forward the data from both WBASN 2 IDs to the doctor's room server and become a blocked mode for WBASN 2. All other solutions proposed for this problem previously are only revocate the cloned node based on its location after the attack was happened. Our proposed method overcome this problem and improves the non-repudiation by entry level check. When the cloned node WBASN 2 tries to enter through node WBASN 10 into the network, WBASN 10 initially check whether similar kind of node is already available or not with the access pointer by verifying the ID. If exist then run the algorithm to find and compare the location of both similar WBASNs with the Message Information Table (MIS) available. The comparison of location is based on its previous history which is available in the same node with respect to previous past time periods t-1, t-2, t-3, …… t-n and with this knowledge the verifying node come to the preliminary conclusion that which node is a original node and other one is duplicated node. Then automatically the duplicated node revocate from the network and communication form that node completely discards by all other nodes. This preliminary detection method improves considerable amount of energy and communication overhead compare to other methods available so far. To ensure the secondary level of verification of the same can be done with other MIT available on other various nodes of the same network by considering them as a witness node. Selection of witness can be done as a random fashion.

Secure, randomized, efficient and distributed protocol: We present a secure algorithm for the detection of clone attacks

```
Rand ←ReceiveBroadcastedRand();
Set time-out Δ;
a→NeigboursOf (a) :< IDa,NeigboursOf (a), IsClaim, (IDa, La,Ta)) >;
While Δ not elapsed and ReceiveMessage(M) do begin
For (i=0;i<n;i++)
If (nodeID[ i] = = nodeID [i+1])
BlockDataFrom (i);
BlockDataFrom(i+1);
For(t=m;t>=0;t - -)
Trusted Node Y= Node
At( Time[ t-1]);
IDy = NodeIDat( Time[ t-1]);
Ty = Time t-1];
Ly = Location(TrustedNodeYat(Time t-1]));
end;
if IsNotCoherent(Ly, Lx)
Iteration 1: RandWitness(IDx, lx, ly, SignedClaim $_x$, SignedClaim $_y$)
 → WitnessNode1
Iteration 2: Response(SignedClaimx, SignedClaimy) →AccessPoint
Iteration 3:(RandWitness(IDx, lx, ly, SignedClaimx, SignedClaimy)
& ! WitnessNode1) → WitnessNode2
if (Claim(WitnessNode1)=Claim(WitnessNode2)))
ExtractClaimValue( );
If(( IDClaim = = IDy) && (LClaim = = Ly))
GrantAccess(Claim(WitnessNode1)) and discard other node;
Else
Goto Iteration 1:
end;
Clear MEM;
```

As a conclusion before making any entry of new node it should be verified with access pointer about its Location and ID by the initial forwarding node. If the same ID exist in the access pointer then the corresponding WBASNs location and IDs to be verified by the initial forwarding node.

Notation used: The following Table 1 shows the notations used throughout in this study.

Security and performance analysis: We investigate clone detection probability during a sequence of iterations. We assume that the adversary has cloned a node, it is also already controlling a subset of S randomly selected other nodes and no mechanism for preventing packet dropping is implemented, so that malicious nodes can stop claim forwarding. Further, we assume that a node (say a) is cloned and one of its clone (say a^0) is randomly deployed within the network area. Moreover, we assume no routing failure and from each neighborhood, exactly one claim message is sent. In RED (17), if just one of these node in the two paths is malicious, detection can fail. In fact, note that the corrupted forwarding node can simply drop the received location claim. The probability that at least one malicious node is present in the paths is:

$$P(A) = 1 - P(A) \text{ where } 0 \le P(A) \le 1$$

Alternatively:

$$P(A) = \frac{\frac{1-(n-g)Cs}{n\,Cs}}{\frac{1-(n-g)Cs}{n\,Cs}}$$

Similarly if ‘S’ is a sample space and A is the any event then probability of the event A is defined as:

$$P(A) = \frac{n(A)}{n(S)}$$

Same way out of ‘n’ nodes selecting ‘g’ no. of witness and the total number of possible ways are:

$$P(A) = \frac{g\,Cw}{n\,Cg} = \frac{g!/(g-w)!w!}{n!/(n-g)!g!}$$
$$= \frac{(g!)2(n-g)!}{(g-w)!w!n!} = \frac{(g!)2(n-g)!}{(g-w)!(w!)\left[(w+1)(w+2).......n\right]}$$

Finally we have to choose the witness from the sample space in the nearby edges or vertices, i.e., The node to select the witness among the available nodes which is far away from the initiating node. If ‘w’ be the witness node near the edge and ‘A’ be one of the witness node among the total ‘n’ nodes, then applying condition probability for more than one event is according to bayes formula:

$$\frac{P\left(\frac{A}{Wm}\right)}{\sum_{m=1}^{n} P\left(\frac{A}{Wm}\right)}$$

$$P\left(\frac{A}{W}\right) = \frac{P(Ai).P\left(\frac{W}{Ai}\right)}{\sum_{m=1}^{n} P\left(\frac{W}{Am}\right).P(Am)}$$

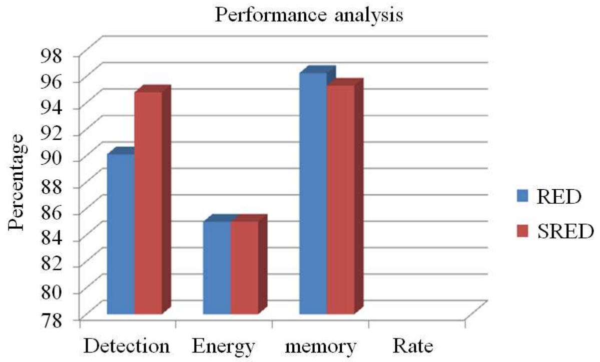


Fig. 3. Comparison of SRED with RED

Table 1: Notations

Notation	Significance
n	Number of nodes in the network
ID_i	The identity of node i
d	Average degree of each node
g	Number of witness nodes
w	Witness node nearby edge or vertices of the sample space
p	Probability a neighbor will replicate location information
H(M)	Hash of M
g	Number of witness selected by each neighbor
l_α	Location node α claims to occupy
s	Sample Space
A	A may be any event

Similarly instead of applying bayes formula for the above condition we can also use the geometrical distribution for the selecting a witness from the sample space is:

$P(A) = p + q.\ p + q.\ q.\ p + \ldots\ldots\ldots\ldots\ldots..$
$P(A) = p.\ q^{x-1}$
Where, x=1, 2, 3… n
For ‘i’ no. iterations
$P(A_i) = [1-q]^i$

The above table shows the comparisons of various protocols with respect to memory and communication overhead in asymptotic notation

The above Fig. 3 shows the comparisons and performance analysis of SRED with RED protocol.

CONCLUSION

The proposed model simulation was carried out using the crossbow kit and the readings were noted using the mote view package as shown in Fig. 4. 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 (ID: 5304, 5325) and the communications were carried on.

The above Fig. 4 shows that the arrangements of 6 six sensor motes with coordinator interface with mote view package. It shows the topology of arrangement and corresponding data values. In our simulation we take Temperature and pressure are the two parameters for various comparisons

In the above Fig. 5 shows the topology arrangement of six sensor motes with gateway or coordinator

In the above Fig. 6 shows the recordings of data from the all the six sensor motes with respect to various time and measurable parameters

In the above Fig. 7 shows the topology arrangement of six sensor motes with gateway or coordinator after making the replication of two motes. In the above topology shows that two nodes are overlapped with other nodes with same SSID.

In the above Fig. 8 shows the recordings of data from the sensor motes with respect to various time and measurable parameters. In the above table shows that two nodes are overlapped with other nodes with same SSID. The readings are continuously changing with overlapped sensor SSID with high and low values. The replicated SSID row shows continuous updation of two sensor nodes, but other SSID rows shows the constant time interval updates. In the above topology shows that two nodes are overlapped with other nodes with same SSID. Here the replicated node enters through other nodes as a multi-hop communication and all other nodes are communicated directly with the gateways

In the above Fig. 10 shows topology arrangement of six sensor motes with gateway or coordinator after making the replication of two motes. In the above topology shows that two nodes are overlapped with other nodes with same SSID. Here the replicated node enters through other nodes as a multi-hop communication and all other nodes are communicated directly with the gateway. The shaded portions shows the light intensity of the replicated node where it was overlapped with original node SSIDs.

In the above Fig. 11 shows the light recording of two nodes with same SSIDs. The X axis taken at a time in ms and the Y axis shows the light intensity in Luminous (LUX). The above result shows the recorded values of node ID 3504 in our simulations.

In the above Fig. 12 shows the temperature recording of two nodes with same SSIDs. The X axis taken at a time in ms and the Y axis shows the temperature. The above result shows the recorded values of node ID 3504 in our simulations.

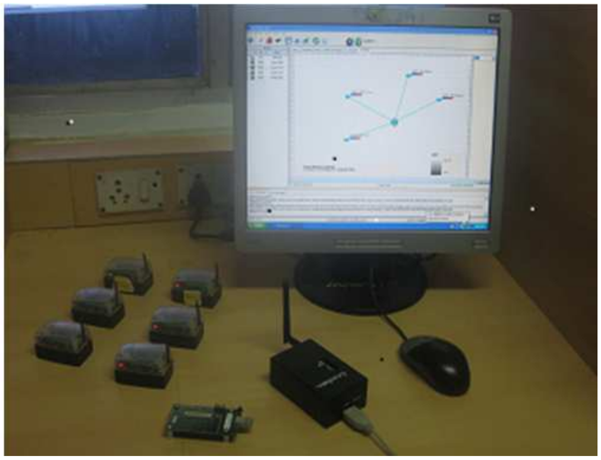
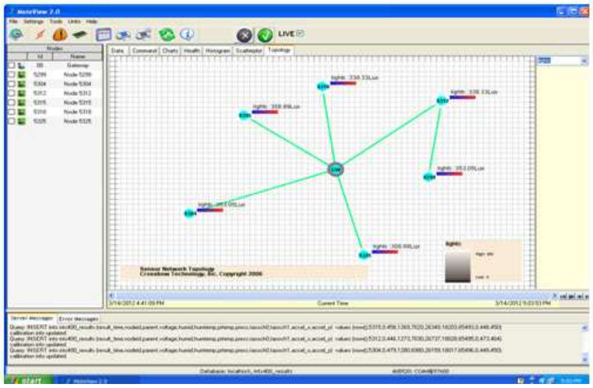
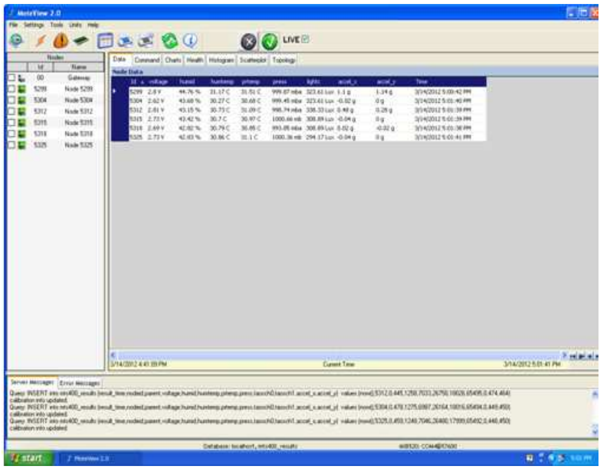


Fig. 4. Cross bow sensor motes with coordinator



MoteView 2.0
File Settings Tools Units Help
LIVE
Data Command Charts Health Histogram Scatterplot Topology
Id Name
00 Gateway
5299 Node 5299
5304 Node 5304
5312 Node 5312
5315 Node 5315
5318 Node 5318
5325 Node 5325
Sensor Network Topology
Crossbow Technology, Inc. Copyright 2006
Server Messages Error Messages
start

Fig. 5. Topology shows the order of sensor motes



MoteView 2.0
File Settings Tools Units Help
LIVE
Data Command Charts Health Histogram Scatterplot Topology
Node Data
Server Messages Error Messages
start

Id	voltage	humid	humtemp	prtemp	press	light	accel_x	accel_y	Time
5299	2.8 V	44.76 %	31.17 C	31.51 C	999.87 mbar	323.61 Lux	1.1 g	1.14 g	3/14/2012 5:00:42 PM
5304	2.62 V	43.68 %	30.27 C	30.68 C	999.45 mbar	323.61 Lux	-0.02 g	0 g	3/14/2012 5:01:40 PM
5312	2.61 V	43.15 %	30.73 C	31.09 C	998.74 mbar	338.33 Lux	0.48 g	0.28 g	3/14/2012 5:01:39 PM
5315	2.73 V	43.42 %	30.7 C	30.97 C	1000.66 mb	308.89 Lux	-0.04 g	0 g	3/14/2012 5:01:39 PM
5318	2.69 V	42.02 %	30.79 C	30.86 C	993.05 mbar	308.89 Lux	0.02 g	-0.02 g	3/14/2012 5:01:38 PM
5325	2.73 V	42.43 %	30.86 C	31.1 C	1000.36 mb	294.17 Lux	-0.04 g	0 g	3/14/2012 5:01:41 PM

Fig. 6: Data table from sensor nodes

In the above Fig. 9 shows topology arrangement of six sensor motes with gateway or coordinator after making the replication of two motes.

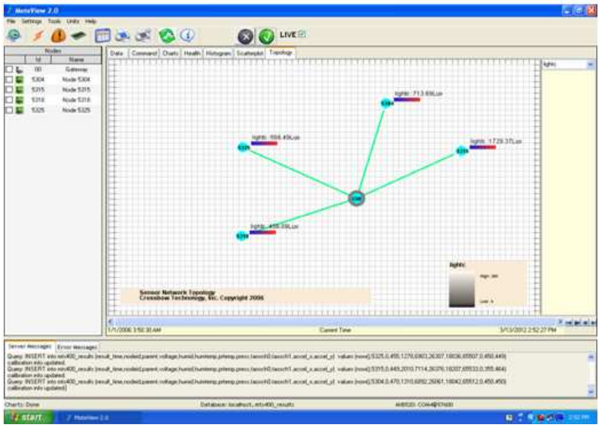
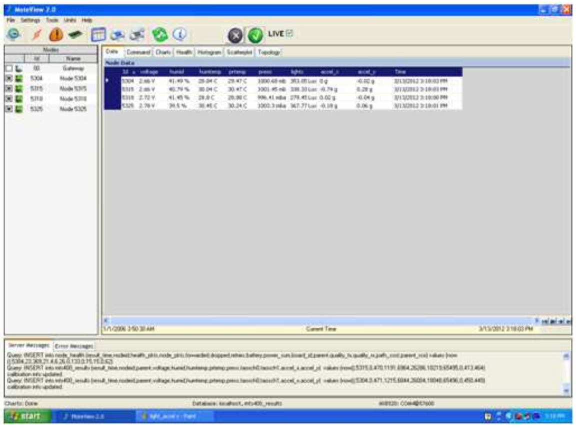

MoteView 2.0
File Settings Tools Units Help
LIVE
Data Command Charts Health Histogram Scatterplot Topology
lights: 713.69Lux
lights: 1729.37Lux
Sensor Network Topology
Crossbow Technology, Inc. Copyright 2006
start

Fig. 7: Topology shows the overlapping (Replicated two sensors were overlapped with other two original sensors)


MoteView 2.0
File Settings Tools Units Help
LIVE
Data Command Charts Health Histogram Scatterplot Topology
Node Data
start

ID	voltage	humid	humtemp	prtemp	press	lights	accel_x	accel_y	Time
5304	2.66 V	41.49 %	29.04 C	29.47 C	1000.48 mb	393.05 Lux	0 g	-0.02 g	3/13/2012 3:10:03 PM
5315	2.66 V	40.79 %	30.04 C	30.47 C	1001.45 mb	338.30 Lux	-0.74 g	0.28 g	3/13/2012 3:10:03 PM
5318	2.72 V	41.45 %	29.8 C	29.80 C	996.41 mba	279.45 Lux	0.02 g	-0.04 g	3/13/2012 3:10:00 PM
5325	2.76 V	39.5 %	30.45 C	30.24 C	1003.3 mba	367.77 Lux	-0.18 g	0.06 g	3/13/2012 3:10:01 PM

Fig. 8: Data table with overlapped IDs

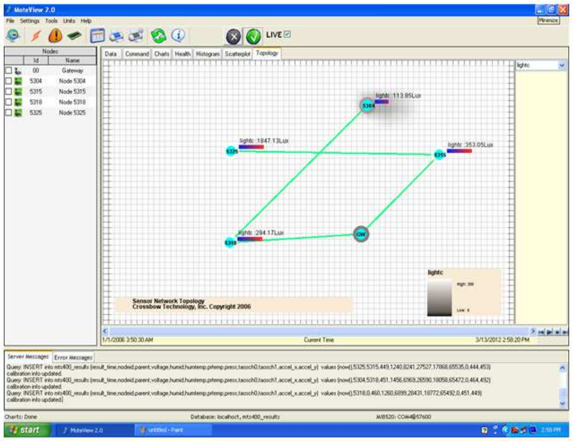

MoteView 2.0
File Settings Tools Units Help
LIVE
Data Command Charts Health Histogram Scatterplot Topology
lights: 113.95Lux
lights: 1847.13Lux
lights: 353.05Lux
lights: 294.17Lux
Sensor Network Topology
Crossbow Technology, Inc. Copyright 2006
start

Fig. 9: Topology shows the entry of replicated node through multihop

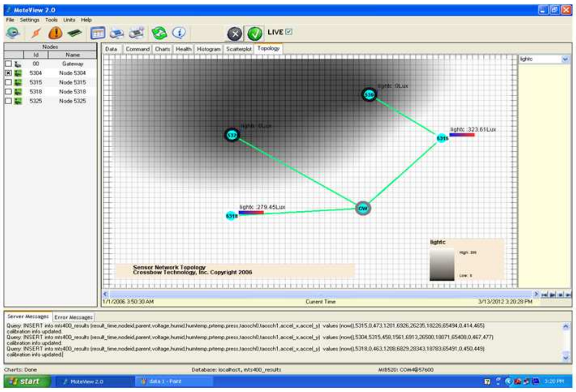

MoteView 2.0
File Settings Tools Units Help
LIVE
Data Command Charts Health Histogram Scatterplot Topology
lights: 323.61Lux
lights: 279.45Lux
Sensor Network Topology
Crossbow Technology, Inc. Copyright 2006
start

Fig. 10: Topology shows light intensity of replicated node

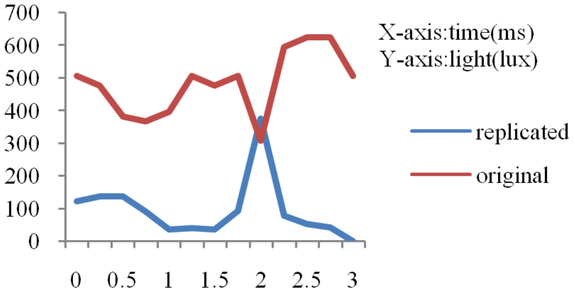


Fig. 11: Graph shows light intensity of replicated nodes for same SSID (ID 3504)

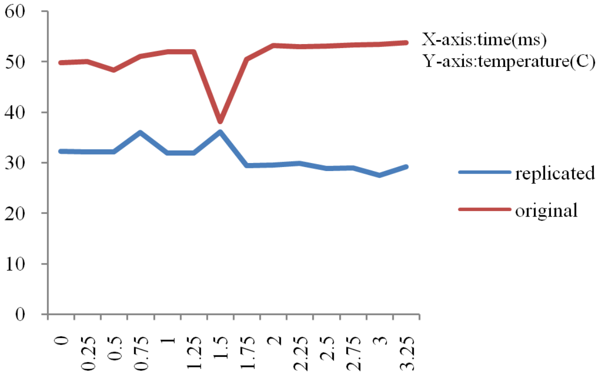


Fig. 12: Graph shows temperature of replicated nodes for same SSID (ID 3504)

ACKNOWLEDGMENT

The researcher are solely responsible for the views expressed in this study, which do not necessarily reflect the position of supporting organizations. This study was partly supported by: AICTE under the project grant scheme RPS and established under the title “Establishing pervasive computing environment.

REFERENCES

Bekara, C. and M. Laurent-Maknavicius, 2007. A new protocol for securing wireless sensor networks against nodes replication attacks. Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Oct. 8-10, IEEE Xplore Press, White Plains, NY., pp: 59. DOI: 10.1109/WIMOB.2007.4390853

Brooks, R., P. Govindaraju, M. Pirretti, N. Vijaykrishnan and M.T. Kandemir, 2007. On the detection of clones in sensor networks using random key predistribution. IEEE Trans. Syst. Man. Cybernetics, Part C: Appli. Rev., 37: 1246-1258. DOI: 10.1109/TSMCC.2007.905824

Choi, H., S. Zhu and T.F.L. Porta, 2007. SET: Detecting node clones in sensor networks. Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks and the Workshop, Sept.17-21, IEEE Xplore Press, Nice, France, pp: 341-350. DOI: 10.1109/SECCOM.2007.4550353

Conti, M., L.V. Mancini and A. Mei, 2011. Distributed Detection of Clone Attacks in Wireless Sensor Networks. IEEE Trans. Dependable Secure Comput., 8: 685-698. DOI: 10.1109/TDSC.2010.25

Conti, M., R.D. Pietro, L.V. Mancini and A. Mei, 2007. A randomized, efficient and distributed protocol for the detection of node replication attacks in wireless sensor networks. Proceeding of the ACM (MobIHoc' 07), pp: 80-89. DOI: 10.1.1.138.6540

Eschenauer, L. and V.D. Gligor, 2002. A Key-Management Scheme for Distributed Sensor Networks. Proceedings of the 9th ACM conference on Computer and Communications Security, Oct. 16-18, ACM, New York, NY, USA, pp: 41-47. DOI: DOI: 10.1145/586110.586117

Ho, J.W., M. Wright and S.K. Das, 2011. Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing. IEEE Trans. Mobile Comput., 10: 767-782. DOI: 10.1109/TMC.2010.213

Menezes, A.J., S.A. Vanstone and P.C.V. Orschot. 1996. Handbook of applied cryptography. 1st Ed., CRC Press, Inc., ISBN:0849385237, pp: 780.

Parno, B., A. Perrig and V.D. Gligor, 2005. Distributed Detection of node replication attacks in sensor networks. Proceeding of the IEEE Symposium on Security and Privacy, May 8-11, IEEE Xplore Press, pp: 49-63. DOI: 10.1109/SP.2005.8

Ratnasamy, S., B. Karp, L. Yin, F. Yu, D. Estrin and R. Govindan *et al*., 2002. GHT: A geographic hash table for data-centric storage. Proceedings of the 1st ACM International Conference on Wireless Sensor Networks and Applications (WSNA' 02), ACM, NY., USA., pp: 78-87. DOI: 10.1145/570738.570750

Xing, K. F. Liu, X. Cheng and D.H.C. Du, 2008. Real-time detection of clone attacks in wireless sensor networks. Proceeding of the IEEE International lst Conference Distributed Computing Systems, 17-20-2008, Beijing, pp: 3-10. DOI: 10.1109/ICDCS.2008.55

Xing, K., X. Cheng, L. Ma and Q. Liang, 2007. Superimposed code based channel assignment in multi-radio multi-channel wireless mesh networks. Proceedings of the 13th Annual International Conference on Mobile Computing and Networking, Sept. 9-14, ACM, New York, pp:15-26. DOI: 10.1145/1287853.1287857

Zhu, B., V.G. K. Addada, S. Setia, S. Jajodia and S. Roy, 2007. Efficient distributed detection of node replication attacks in sensor networks. Proceedings of the 23rd Annual Computer Security Applications Conference, Dec. 10-14, IEEE Xplore Press, Miami Beach, FL., pp: 257-267. DOI: 10.1109/ACSAC.2007.26