Journal of Computer Science 2012, 8 (11), 1880-1888
ISSN 1549-3636

doi:10.3844/jcssp.2012.1880.1888 Published Online 8 (11) 2012 (http://www.thescipub.com/jcs.toc)

TRUST BASED NODE REPLICATION ATTACK DETECTION PROTOCOL FOR WIRELESS SENSOR NETWORKS

V. Manjula and C. Chellappan

Department of Computer Science and Engineering,
College of Engineering Guindy, Anna University, Tamil Nadu, India

Received 2012-06-07, Revised 2012-09-13; Accepted 2012-11-05

ABSTRACT

The harmful attack against Wireless Sensor Networks (WSN) is Node Replication attack, where one or more node(s) illegitimately claims an identity, are also called clone attack due to identity theft. The Node replication attack can be exceedingly injurious to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, This study proposes a method Randomized and Trust based witness finding strategy for replication attack detection mechanisms in wireless sensor networks (RTRADP) with trust factor. Resilient to malicious witness and increased detection rate by avoiding malicious witness selection. Performances are compared with the existing witness finding approach and how the malicious witness drops the claim without processing and how those malicious witnesses are avoided with trust based approach.

Keywords: Wireless Sensor Networks (WSN), Security, Clone, Node Replication Attack, Wireless Sensor Network, Randomized and Trust

1. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate in order to achieve a common goal. Sensor nodes operate in hostile environments such as battle fields and surveillance zones. Due to their operating nature, WSNs are often unattended, hence prone to several kinds of novel attacks.

The mission-critical nature of sensor network applications implies that any compromise or loss of sensory resource due to a malicious attack launched by the adversary-class can cause significant damage to the entire network. Sensor nodes deployed in a battlefield may have intelligent adversaries operating in their surroundings, intending to subvert damage or hijack messages exchanged in the network. The compromise of a sensor node can lead to greater damage to the network. The resource challenged nature of environments of operation of sensor nodes largely differentiates them from other networks. All security solutions proposed for sensor networks need to operate with minimal energy usage, whilst securing the network.

We classify sensor network attacks into three main categories (Baig, 2008). Identity attacks, routing attacks and network intrusion.

Table 1 shows the attack taxonomy in wireless sensor network. The identity attacks are Sybil attack and clone (Replication) attack. In a Sybil attack, the WSN is subverted by a malicious node which forges a large number of fake identities in order to disrupt the network's protocols. A node replication attack is an attempt by the adversary to add one or more nodes to the network that use the same ID as another node in the network.

Routing attack intend to place the Rogue nodes on a routing path from a source to the base station may attempt to tamper with or discard legitimate data packets. Some of the routing attacks are Sinkhole Attack, False

Corresponding Author: Manjula, V., Department of Computer Science and Engineering, College of Engineering Guindy, Anna University, Tamil Nadu, India

routing information attack, Selective forwarding attack and Wormholes. The adversary creates a large sphere of influence, which will attract all traffic destined for the base station from nodes which may be several hops away from the compromised node which is known as sinkhole attack. False routing attack means that injecting fake routing control packets into the network. Compromised node may refuse to forward or forward selective packets called as Selective forwarding attack. In the wormhole attack, two or more malicious colluding nodes create higher level virtual tunnel in the network, which is employed to transport packets between the tunnel end points.

In this study we are concentrating on an identity attack called replication attack where one or more nodes illegitimately claim an identity of legitimate node and replicated in whole WSN network. Reason for choosing this attack is that it can form the basis of a variety attacks such as Sybil attack, routing attacks and link layer attacks. also called as denial of service attacks. The detection of node replication attacks in a wireless sensor network is therefore a fundamental problem. A few centralized and distributed solutions have recently been proposed and discussed in related work section. However, these solutions are not satisfactory, they are energy and memory demanding: A serious drawback for any protocol that is to be used in resource constrained environment such as a sensor network. Further, they are vulnerable to specific adversary models which is discussed in our study.

1.1. Related Work

The replication attack detection mechanism can be classified as prevention and detections schemes. Prevention scheme that inherently forbid cloned nodes to join network. In this scheme the identity-based cryptography-nodes private keys are bounded by both their identities and locations (Brooks *et al*., 2007). The detection protocol can be classified as centralized and distributed protocols.

A centralized protocol (Parno *et al*., 2005) relies on a centralized Base Station (BS). Each node sends a list of its neighbors and their claimed locations to the BS. The BS can then examine every neighbor list to look for replicated nodes. Finally the base station can revoke the replicated nodes by flooding the network with an authenticated revocation message. This solution has a single point of failure and it requires a high communication cost. Further, nodes close to the BS will exhaust their power earlier than others because of tunnelling effect. Local protocol is also a kind of solution for detecting replication attacks. A voting mechanism is used on a node's neighbors in (Heesook *et al*., 2007). The neighbors can reach a consensus on the legitimacy of a given node. But those protocols fail to detect replicas two or more hops away from each other.

Several distributed detect protocols were proposed for detecting node replication attacks. We adopt some notations in (Sei and Honiden, 2008; 2009). In these protocols, every node broadcasts its ID and location to one-hop neighbors. We call this message as a claim and the node that broadcasts a claim is called as claimer node. Upon receiving a claim message, each neighbor with probability p_f forwards the claim message to a set of nodes called witnesses. A neighbor node which forwards a claim, we call it a reporter node. If a witness node receives two or more claim messages containing the same ID but different locations, the witness node detects a replication attack. The first distributed node replication detect protocol was proposed in (Parno *et al*., 2005). Two distributed protocols were proposed: Randomized Multicast (RM) and Line Select Multicast (LSM). RM protocol propagates claim message to randomly selected witness nodes. When a claimer node broadcasts its location claim, each of its neighbors with probability p_f propagates the claim to a set of randomly selected witness nodes. According to the Birthday Paradox, at least one node is likely to receive conflicting location claims of a particular node.

Table 1. Attack taxonomy

Attacks	Description	Examples
Identity attack	Identity attacks intend to steal the identities of legitimate nodes operating in the sensor network	1. Sybil Attack 2. Replication Attack
Routing attack	Routing attack intend to place the Rogue nodes on a routing path from a source to the base station may attempt to tamper with or discard legitimate data packets.	3. Sinkhole attack 4. False routing information attack 5. Selective forwarding attack 6. Wormhole attack
Network Intrusion	Unauthorized access to a system by either an external perpetrator, or by an insider with lesser privileges.	

Each neighbor needs to send O (√ n) messages, where n is the number of sensors in the network. LSM protocol behavior is similar to RM but introduces a modification that achieves a noticeable improvement in terms of detection probability and communication cost. When a node broadcasts its location claim, every neighbor forwards this claim with probability p_f. If a neighbor forwards the claim, it randomly selects a fixed number *g* witness nodes and sends the signed claim to all the *g* nodes. The number of witness nodes *g* can be much smaller than in RM. Every node that is routing the claim message must to check the signature of the claim, then store the signed claim and check for coherence with the other location claims stored within the same detect iteration. So, the forwarding nodes are also witness nodes of the claimer node. Node replication is likely detected by the nodes on the intersection of two route paths that originate from different locations by the same ID.

Two distributed replication detect protocols SDC and P-MPC were proposed in (Zhu *et al*., 2007). The network is considered to be a geographic grid in the study. In the SDC protocol, a geographic hash function is used to uniquely and randomly map a node's identity to one of the cells in the grid. The location claim message is forwarded to the mapping cell. When the first copy of the location claim arrives at the destination cell, the location claim is flooded within the cell. The nodes in the cell randomly become witness nodes. In P-MPC, to increase the reliability to a large amount of replication nodes, a node's identity is mapped to several cells in the grid. So, the candidate witness nodes for one node are nodes of several cells. Smart attacker can predict and subvert the witnesses with the predefined locations or cells.

An efficient, distributed protocol RED was proposed in (Conti *et al*., 2007; 2010). Different from RM and LSM, all reporter nodes of a particular claimer node α would choose the same g witness nodes for α, while in RM and LSM, each reporter node randomly determines a set of witness nodes. In RED protocol, the witness nodes' locations are determined by the claimer node ID and the seed rand. A trusted entity broadcasts a seed to the whole network in each detect iteration. Because the seed changes in every detect iteration, the attacker cannot anticipate the witness nodes. As described above, each neighbor node of a claimer node with probability p_f becomes reporter node and forwards the claim message to *g* witness nodes. The larger p_f is, the higher the success detect rate is and a claimer node tends to have more reporter nodes.

Randomwalk (Zeng *et al*., 2010), strategy avoids smart attacker who predicts the critical witness, because it naturally distributes the responsibility of witness node selection to every passed node of random walks and then adversaries cannot easily find out the critical witness nodes. The first protocol, RAndom WaLk (RAWL), starts several random walks randomly in the network for each node a and then selects the passed nodes as the witness nodes of node a. RAWL analysis shows that O(√n log n) walk steps are sufficient to detect clone attacks with high probability. The second protocol, Table-assisted RAndom WaLk (TRAWL), is based on RAWL and adds a trace table at each node to reduce memory cost. Usually the memory cost is due to the storage of location claims; in TRAWL each node only stores O(1) location claims now (although the size of the trace table is still O(√n log n), the size of a table entry is much smaller than the size of a location claim).

In witness finding strategy (Manjula and Chellappan, 2011a; 2011b), randomness is important criteria to avoid prediction of future witnesses. If the adversary knew future witnesses, they subvert the nodes, in such a way that attack would go undetected. But, there is a probability that malicious node itself chosen as witness due to randomness. In Random Mulicast (RM), Line Selected Multicast (LSM) and RED uses Random selection of witnesses over whole network and the detection rate in RM and LSM algorithm tightly dependent on no. of witness node selection O(√n). Witness node identity randomly selected from the node that are located within the geographically limited region (referred to as cell) in SDC and P-MPC. In these approaches, they assumed that chosen witnesses are benevolent.

The problem with randomized witness selection is:

- If Randomly chosen witness itself is malicious then what will be the assurance of clone attack detection?
- And how can be avoided those witnesses?

So, here transaction information is used to decide the behavior of witness like selfishness, consistency of node based data validity and battery life. Before forwarding claim by the neighbor node, it checks the trustworthy of witnesses, since the randomly chosen witness nodes may be malicious or cloned node itself. Trust of a witness node is evaluated with selfishness and consistency factors. The battery power of node is considered to evaluate the Trust as it affects selfishness behavior.

2. MATERIALS AND METHODS

2.1. Network and Adversary Models

2.1.1. Notations

The description of parameters given in the **Table 2**: Notations are used in the following sections to illustrate the protocol feature.

2.2. Network Model

We assume nodes are uniformly distributed in the deployment field. We assume nodes know their own locations by various localization alogorithms (Savvides *et al*., 2001; Capkun and Hubaux, 2006). We assume nodes are stationary, at least during the execution of replica detection protocol. Each node a has a private key K-1 (a) and can use the private key to sign its location claim. Other nodes are also able to verify the signature. Now several public key libraries for sensor networks are available. We also assume the communications between any two nodes are protected by pair wise keys which is same as previous works (Parno *et al*., 2005; Heesook *et al*., 2007; Zhu *et al*., 2007; Conti *et al*., 2007; Xing *et al*., 2008). We assume that the adversary cannot create new IDs for replicas with some key management schemes already provides such property (Chan *et al*., 2003; Zhu *et al*., 2003) and other measures (Newsome *et al*., 2004) can also be introduced into key management schemes to enforce such property (e.g., mapping ID to the indices of keys with a one-way function). Each node knows their neighbours information about the legitimacy of the location and data compared with their own and also selfishness or normality of communication behaviour.

2.3. Adversary Model

The adversary can launch a clone attack: he compromises a few nodes (Zhu *et al*., 2007) and uses the cryptographic information obtained from the compromised nodes to produce replicas and then inserts the replicas into the network. The compromised nodes and replicas are fully controlled by the adversary and can communicate with each other at any time. Also, same as previous protocols (Heesook *et al*., 2007; Xing *et al*., 2008), we assume nodes controlled by the adversary still follow the replica-detection protocol, since the adversary always wants to keep him unnoticed to others. They play hide and seek, the adversary may not participate in the regular detection or gives the fake location information. And also the adversary will try to protect its replicas by dropping (or) without forward location claim of legitimate node. Since, if any replicas are detected, besides starting a revoke process to revoke the replicas and behave as selfish node, without forwarding data to required location. This behavior can be quantified and evaluated with Trust model.

2.4. Trust Model

Each node evaluates trustworthiness of its neighbor nodes behavior by cross checking the neighbor nodes' redundant sensing data with its own result by overhearing. The flow chart illustrated in the **Fig. 1** represents the trust model. The Trust model evaluate the trust worthiness and each node maintains the details of neighbors behavior with consistency count, inconsistency count, sensing success and sensing failure. Each node updates neighbor behavior table, when valid/legitimate data, then increment the consistency count and if not valid, then increment the inconsistency count, since malicious node may inject false data. Using sensing success and sensing failure, find out selfishness and normality of node, since malicious node may not participate in the detection process as well as regular activity to save power, which asses the node behavior. Trust model also includes the battery power, since less power device may not in detection process and selfishness behavior related the power. From these detail we quantify the node behaviour with consistency factor, Sensing Factor and battery power and to compute the trust factor and with following trust quantification process and computation process (Hur *et al*., 2005).

Table 2. Notations

Notation	Description
n	Number of nodes in the network
d	Average degree of each node
p	Probability a neighbor will forward location claim
g	Number of witness nodes selected by each neighbor
La	Location node a claims to occupy
Ka	a's public key
K^{-1} a	a's private key
{M} K^{-1} a	a's signature on Message M
H (M)	Hash of Message M
MACK (M)	Message authentication code of M with key K
C_i	Consistency value of node i, where 1< i < k
CS_i	Consistent sensing count of node i
IS_i	Inconsistent sensing count of node i
Si	Sensing communication value of node i
SSi	Sensing success count of node i
SFi	Sensing failure count of node i
B_i	Battery life value ($-1 \leq B_i \leq +1$) – represents lifetime of sensor node
W_1, W_2, W_3, Wi	Wi -Weight which represents importance of each factor from 0(unimportant) to 1 (most important)
Ti	Trust value for node i
R	No. of replicas
G	Pseudo random function

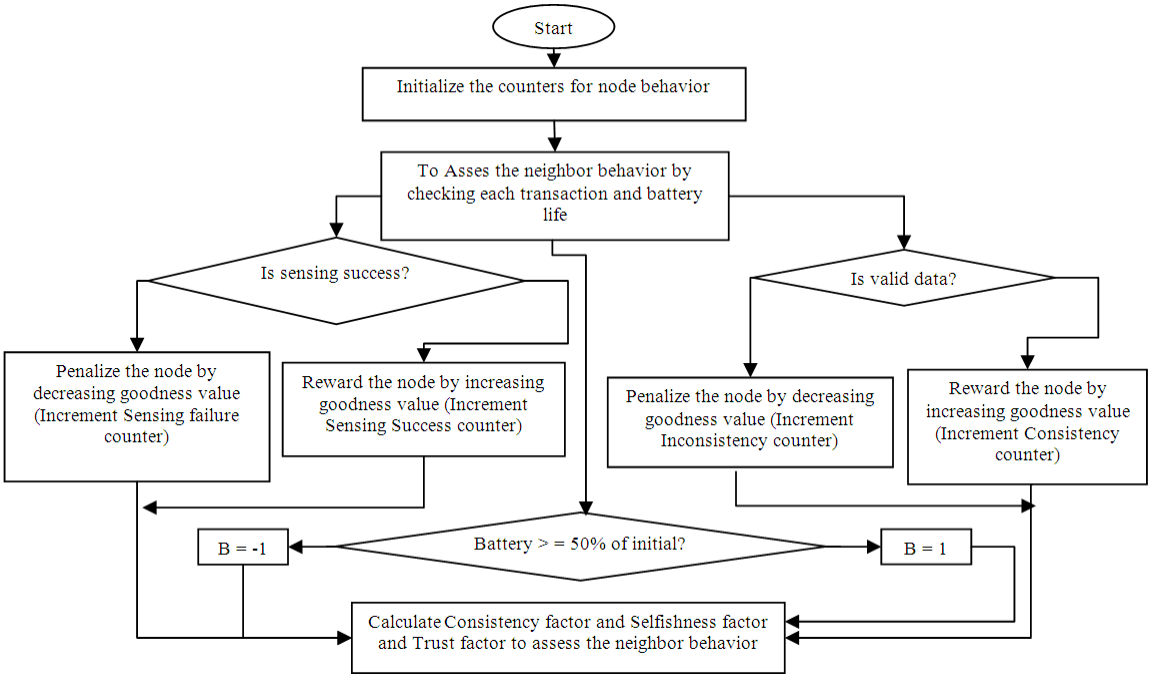


Fig. 1. Flow chart for Trust model

2.5. Trust Quantification Process

i) Consistency value ($-1 \leq Ci \leq +1$) This factor represents a level of consistency or validity of a node. Equation 1 evaluates the level of consistency of the node by computing the percentage difference among Consistency count and Inconsistency count:

$$C_i = \frac{CS_i - IS_i}{CS_i + IS_i} \quad (1)$$

ii) Sensing Communication value ($-1 \leq Si \leq +1$) – represents level of selfishness and normality of node which is calculated by the Eq. 2:

$$S_i = \frac{SS_i - SF_i}{SS_i + SF_i} \quad (2)$$

iii) Battery value ($-1 \leq B_i \leq +1$) – represents lifetime of sensor node. Battery Energy of node is less than 50 % of initial energy, then B_i=-1 else $B_{i=}$+1

2.6. Trust Computation

Ti = Trust value for node i is computed by Eq. 3 equation. If $B_i \neq -1$:

$$Ti = \frac{W_1 C_i + W_2 S_i + W_3 B_i}{\sum_{i=1}^{3} W_i} \quad (3)$$

2.7. Protocol Description

Our protocol can be scheduled to run periodically. The protocol initialized by generating and broadcasting random seed by centralized base-station (or satellite). At a high level, Randomized Trust based Replication Attack Detection Protocol (RTRADP) works with following steps in each execution:

- After receiving seed, each node broadcasts a signed location claim. Each of the node's neighbours probabilistically forwards the claim to some pseudo-randomly selected nodes
- Before forwarding the claim message, collects the trust of randomly selected node from their neighbours and compares with the threshold
- If greater than are equal to threshold of randomly selected node, it will be chosen as witness node and forwards a message containing the claim
- The witnesses will store the claim and if any witness receives different location claims for a same node ID, it can use these claims to revoke the replicated node. An example is shown in **Fig. 2**

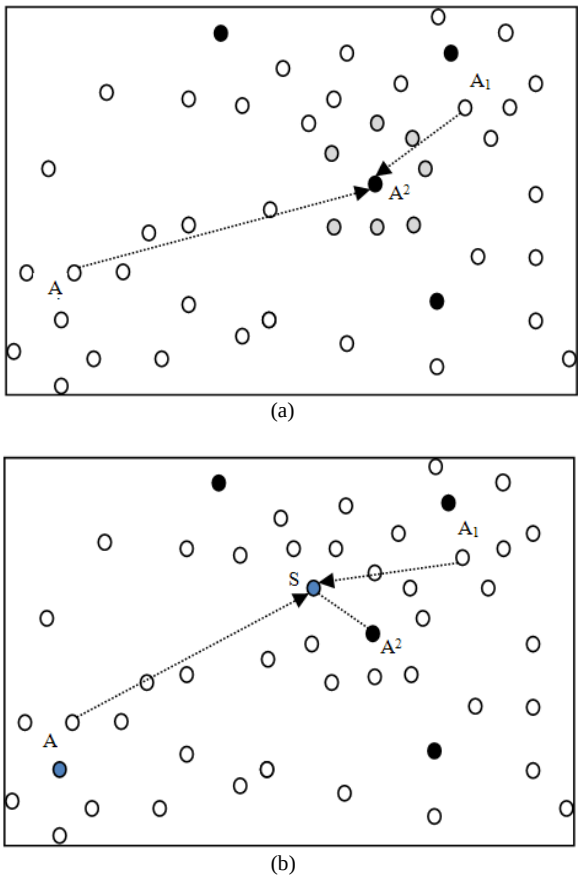


Fig. 2. (a) Existing Random Witness Approach (b) Proposed Approach

In **Fig. 2a** illustrates scenario of the existing random witness protocols, it may chooses the malicious node (marked as black) A^2 as random witness. This node definitely subverts protocol as well as the network without detecting replicas. In our approach that malicious node is avoided from choosing as witness by the trust factor collected from their neighbors (grey colour). This scenario illustrated in the **Fig. 2b**, the protocol avoids the node A^2 and chooses the node S.

We here describe the protocol more specifically. The protocol initialized with broadcasting random seed by central control may be base station or by cluster heads. It should reach the whole network. After receiving seed and set the timeout Δ, the each node a, broadcasts a signed location claims to its neighbors. The claim has such a format: $< ID_a, l_a, \{H(ID_a||l_a)\} K^{-1}_a>$, where l_a is *a*'s location (e.g., location (x,y) in 2D) and || is the concatenation. When hearing the claim, each neighbor verifies the signature and checks the plausibility of l_a (e.g., the distance between two neighbors cannot be bigger than the transmission range). Assume the degree of neighbor d and then with forwarding probability p, each neighbor pseudo-randomly selects *g* nodes (or *g* locations) and gets trust factor from their neighbors of each g nodes and finds cumulative trust factor and compares with the threshold (T_{thresh}). If it satisfies with threshold then forward the claim to the *g* nodes (or nodes closest to the chosen g locations). The trust quantification and computation has been discussed trust model of previous section. Here geographic routing (e.g., GPSR) used to get trust factor and also to forward claim. Each chosen node that receives the claim of a, first verifies the signature. Then it stores the claim and becomes a witness node of a. When a node finds a collision (two different location claims with a same node (ID), the node will broadcast the two conflicting. Conti *et al*. (2007) the authors claimed that choosing location is better than choosing node ID since the available node IDs in the network may be dynamic.

The entire nodes selects witness from the deterministic set; this will be random and vary at each protocol run by random seed. Equation 4 gives the Pseudo Random function for witness selection with the parameters are seed, number of nodes and number of witnesses.

$$G = F(seed, n, g) \quad (4)$$

2.9. Security Analysis

The detection rate of node replication attack depends on witness legitimacy and also neighbors legitimacy. Probability of detection of attack P(D), is high when at least one common witness chosen by the neighbor of both legitimate and replicated node and also it should be honest(not malicious-M′) witness. Let us consider the event space(I) with following four disjoint events:

Case1: Honest(H) and Noncommon(C′) witness
Case2: DisHonest(H′) witness but Common witness(C)
Case3: DisHonest(H′) and Noncommon witness(C′)
Case4: Honest(H) and Common(C) witness

Then, P(I) is:

$P(I)=P(H\cap C')+P(H'\cap C)+P(H'\cap C')+P(C\cap H)$ and

Probabality of attack detection P(D) depends on case 4.

$P(D)=P(C\cap H)= P(C/H)P(H)$

The events that undetecting attack durings the Case1, Case2 and Case3. Assume that Probability of event undetecting attack is P(U) .

$P(U) = P(H \cap C') + P(H' \cap C) + P(H' \cap C')$

$P(U) = P(C'/H)P(H) + P(C/H')P(H') + P(C'/H')P(H')$

$P(U) = P(C') + P(C/H')P(H')$

since, $P(C') = P(C'/H)P(H) + P(C'/H')P(H')$ and $P(C/H') = 1$, because not honest(H′)witness (ie., malicious witness) drop the claim and event of undetection become sucess. So, rewrite the equation as:

$P(U) = P(C') + P(H')$

$P(D) = 1 - P(U) = 1 - P(C') - P(H')$

Probability of undetection is sum of Probability of non common witness selection P(C') and probability of dishonest witness P(H'). So the probability of non-common witness is P_{ND1} in RM (Parno *et al*., 2005) is Eq. 5:

$$P(C') = P_{ND1}$$
$$P_{ND1} = e^{-\frac{(pdg)^2}{n}\left(\frac{R(R-1)}{2}\right)} \quad (5)$$

The attack will be detected when at least one common witsesses chosen by the neighbors of clone provided that node is honest witness.

Consider the Probability of choosing not honest witness or choosing malicious witness is a Poisson process. Let λ % of malicious nodes out of n nodes. λ = R, is number of replicas. Probability of detection is depends on atleast one honest witness choosen. P_{none}(Honest) = P(All Malicous(M) Witness out of p.d.g trials) Eq. 6:

$$P_{none}(honest) = \frac{e^{-R}R^{p.d.g}}{(p.d.g)!} \quad (6)$$

For 0< = M < = p.d.g trials of witness selection.

Assume average neighbor degree (d) = 30, g = 1, p = 0.1 and R = 5. Then probability of zero malicious witness node selection: where p.d.g = 0, then $\frac{e^{-R}R^0}{(0)!}$ = 0.0067 and p.d.g = 3, then P_{none} (Honest) i.e., all are malicious of p.d.g. trials = 0.14037. Assume that there is (at least one) always common witness. Then P(C') = 0, since Non-detection depends on probability dishonest witness selection.

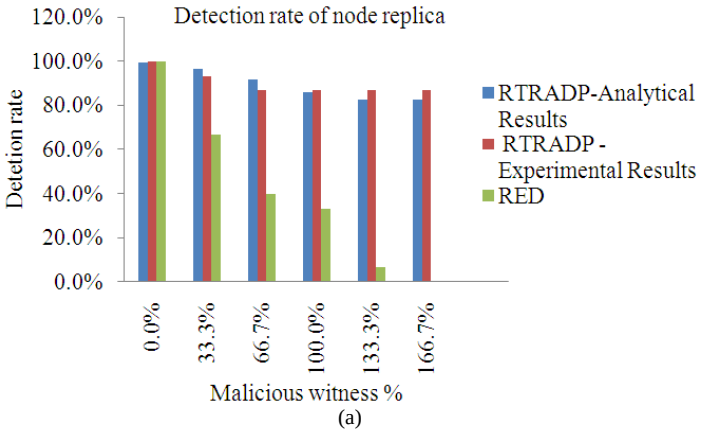
3. RESULTS AND DISCUSSION

3.1. Results

3.1.1. Simulation Setup and Assumptions

In our simulations, we randomly deploy 4000 nodes within a 1000×1000 m square. Such that the nodes are distributed in the network area uniformly at random.

The transmission range is set to 50 m. Assume that all the forwarding nodes before the witnesses are honest; since the malicious nodes can prevent clone detection if they are in the path before the witness. We also set no. of witnesses g = 1 and forwarding probability p = 0.1 for both RED and RTRADTP protocols. This means that this two protocols send the same number of location claims per node (on the average). With above setup 5 replicas considered with different percentage of malicious witness selection out of p.d.g witnesses i.e., 0,1, 2, 3... malicious witness nodes and with the $Trust_{thres}$ = 75%. Assumed Weightage of Consistency factor (Ci), Communication factor (Si) and Battery lfe value are 0.35, 0.35 and 0.30 respectively.



(a)

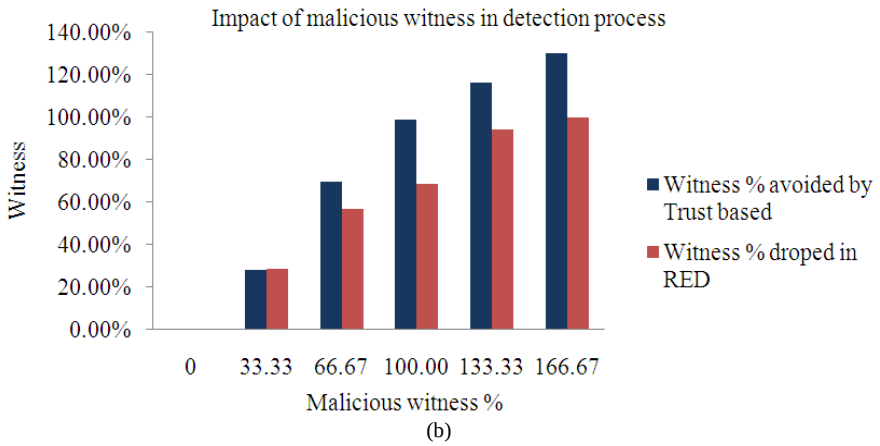


Fig. 3. (a) Detection Rate (b) Impact of malicious witness in detection processs

There will be the chances of selecting the cloned node itself as witness or clone compromises the witness. Those malicious witnesses prevent the detection. This will be avoided in our approach with the trust factor. **Figure 3a** shows that the malicious witness affects the detection rate in RED and it is reduced to 0% when perentage of clones act as witness (malicious) increases. In our approach (RTRADP), those malicious witnesses are avoided and the detection rate of experimental results is 100-86.7% and also maintains almost to the detection rate of analytcial results 99.3-85.9%. During the node replication attack detection process, the **Fig. 3b** shows percentage of witness drops the claim in RED and percentage of witness avoided in our approach with trust against the malicious witness percentage.

4. CONCLUSION

In this study, randomized and trust based detection mechanism for replication attack which is resilient to the malicious witness chosen have been discussed. Performance compared Analytically and Experimentally with the existing witness finding approach, how the malicious witness drops the claim without processing and how those malicious witnesses avoided with trust based approach. our approach resilient detection process by avoiding malicious witnesses when compared to the existing witness finding approach. The proposed RTRADP method avoids malicious witnesses and maintains the detection rate of 100 to 86.7% when malicious witness percentage increases. But in existing approach detection rate is reduced from 100 to 0%, with increasing the malicious witness percentage. For future work, to find Malicious clone among the clones and revoke only malcious clones instead of all the clones.

5. ACKNOWLEDGEMENT

The researchers would like to thank NTRO sponsored Collaborative Directed Basic Research- Smart and Secure Environment Project Lab for providing computing facilities and UGC for financial support by providing fellowship.

6. REFERENCES

Baig, Z.A., 2008. Distributed denial of service attack detection in wireless sensor networks. Monash University.

Brooks, R., P.Y. 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

Capkun, S. and J.P. Hubaux, 2006. Secure positioning in wireless networks. IEEE J. Sel. Areas Commun., 24: 221-232. DOI: 10.1109/JSAC.2005.861380

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. Proceeding IEEE Symposium on Security and Privacy, May 11-14, IEEE Xplore Press, pp: 197-213. 10.1109/SECPRI.2003.1199337

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. Proceedings of the 8th ACM International Symposium on Mobile ad Hoc Networking and Computing, Sept. 09-14, ACM Press, Montreal, Canada, pp: 80-89. DOI: 10.1145/1288107.1288119

Conti, M., R.D. Pietro, L.V. Mancini and A. Mei, 2010. Distributed detection of clone attacks in wireless sensor networks. IEEE Trans. Depedable Secure Comput., 8: 685-698. DOI: 10.1109/TDSC.2010.25

Heesook, C., Z. Sencun, L. Porta and F. Thomas, 2007. SET: Detecting node clones in sensor networks. Proceedings of the 3rd International Conference on Security and Privacy in Communications Networks and the Workshops, Sept. 17-21, IEEE Xplore Press, Nice, France, pp: 341-350. 10.1109/SECCOM.2007.4550353

Hur, J., Y. Lee, S.M. Hong and H. Yoon, 2005. Trust management for resilient wireless sensor networks. Proceedings of the 8th International Conference on Information Security and Cryptology, Dec. 1-2, Springer Berlin Heidelberg, Seoul, Korea, pp: 56-68. DOI: 10.1007/11734727_7

Manjula, V. and C. Chellappan, 2011a. The replication attack in wireless sensor networks: Analysis and defenses. Adv. Netw. Commun., 132: 169-178. DOI: 10.1007/978-3-642-17878-8_18

Manjula, V. and C. Chellappan, 2011b. Replication attack mitigations for static and mobile WSN. Int. J. Netw. Security Appli., 3: 122-133. DOI: 10.5121/ijnsa.2011.3210

Newsome, J., E. Shi, D. Song and A. Perrig, 2004. The sybil attack in sensor networks: Analysis and defenses. Proceedings of the 3rd International Symposium Information Processing in Sensor Networks, Apr. 26-27, ACM Press, Berkeley, CA, USA., pp: 259-268. DOI: 10.1145/984622.984660

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

Savvides, A., C.C. Han and M. Srivastava, 2001. Dynamic fine-grained localization in Ad-Hoc networks of sensors. Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, Jul. 16-21, ACM Press, Rome, Italy, pp: 166-179. DOI: 10.1145/381677.381693

Sei, Y. and S. Honiden, 2008. Distributed detection of node replication attacks resilient to many compromised nodes in wireless sensor networks. Proceedings of the 4th Annual International Conference on Wireless Internet, Nov. 17-19, ACM Press, Maui, HI, USA.

Sei, Y. and S. Honiden, 2009. Reporter node determination of replicated node detection in wireless sensor networks. Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, Jan. 15-16, ACM Press, Suwon, Republic of Korea, pp: 566-573. DOI: 10.1145/1516241.1516340

Xing, K., F. Liu, X. Cheng and D.H.C. Du, 2008. Real-time detection of clone attacks in wireless sensor networks. Proceedings of the 28th International Conference on Distributed Computing Systems, Jun. 17-20, IEEE Xplore Press, Beijing, pp: 3-10. DOI: 10.1109/ICDCS.2008.55

Zeng, Y. J. Cao, S. Zhang, S. Guo and L. Xie, 2010. Random-walk based approach to detect clone attacks in wireless sensor networks. IEEE J. Sel. Areas Commun., 28: 677-691. DOI: 10.1109/JSAC.2010.100606

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

Zhu, S., S. Setia and S. Jajodia, 2003. LEAP: Efficient security mechanisms for large-scale distributed sensor networks. Proceedings of the 10th ACM Conference on Computer and Communications Security, Oct. 27-30, ACM Press, Washington, DC, USA., pp: 62-72. DOI: 10.1145/948109.948120