IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. IV. (Jul.-Aug. 2017), PP 68-73
www.iosrjournals.org

On The Node Clone Detection Using Hashing In WSN

*Garikapati.Divya [1], L V Krishna Rao [2]
[1]*M.Tech.IV Sem.(CSE) Lakireddy Balireddy College of Engineering, Mylavaram*
[2]*Assistant Professor, CSE Department, Lakireddy Balireddy College of Engineering, Mylavaram*
*Corresponding Author: *Garikapati.Divya*

Abstract: *Wireless sensor networks accommodate a whole lot to thousands of sensor nodes and are wide employed in civilian and security applications. One in every of the intense physical attacks faced by the wireless sensor network is node clone attack. So node clone detection protocols area unit introduced via distributed hash table and arbitrarily directed exploration to detect node clones. The previous primarily based on a hash table value that is already distributed and provides key based facilities like checking and caching to observe node clones. The later one is exploitation probabilistic directed forwarding technique and border determination. The simulation results for storage consumption, communication value and detection chance is completed exploitation NS2 and obtained arbitrarily directed exploration is that the best one having low communication value and storage consumption and has smart detection chance.*

Key Words: *wireless Sensor network, clones, DHT, RDE.*

Date of Submission: 12-07-2017 Date of acceptance: 05-08-2017

I. Introduction

A Wireless sensor Network or WSN is meant to be made from a large variety of sensors and a minimum of one base station.wsn has been variety of applications like environment monitoring and object tracking,etc[2][3].In wsn the sensors are smaller size and lower price with many constraints like the battery power, communication range and memory. because of their nature the adversary prone to different attacks[4][5][6][7][8]. Therefore, an adversary may duplicate captured sensors and deploy them in the network to launch a variety of attacks.This attack is referred to as the clone attack[9][12]. since the clone has rightful information (code and cryptographic material),it may participate in the network operation in the same way as a non compromised node; hence clone node can launch a variety of attacks.

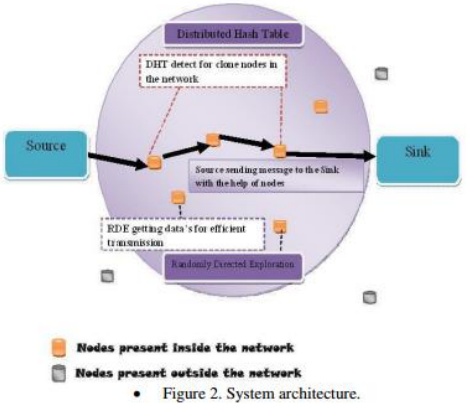
Our contribution In this paper, besides the clone detection probability, we tend to in addition believe energy consumption and memory storage among the design of clone detection protocol, i.e., an energy- and memory-efficient distributed clone detection protocol with random witness alternative theme in WSNs[1].Our protocol is applicable to general densely deployed multi-hop WSNs, where adversaries would possibly compromise and clone sensor nodes to launch attacks[2][3]. We prolong the analytical model by evaluating the vital data buffer of ERCD protocol and by together with experimental results to support our theoretical analysis. Energy-Efficient Ring based totally Clone Detection (ERCD) protocol[1].We find that the ERCD protocol can balance the energy consumption of sensors at totally different locations by distributing the witnesses all over WSNs except non-witness rings, i.e., the adjacent rings round the sink, that should not have witnesses.After that, we tend to acquire the optimum vary of non-witness rings based on the perform of energy consumption. Finally, we tend to derive the expression of the required data buffer by using ERCD protocol, and show that our projected protocol is scalable as a result of the required buffer store depends on the ring size solely.

II. Detection Protocols

Based on the detection methodologies, we classify two novel node clone detection protocols.
1. Distributed hash table (DHT)
2. Randomly directed exploration (RDE)

A. DISTRIBUTED HASH TABLE (DHT): DHT through which a not fully centralized, key-based caching and checking process is constructed to capture cloned nodes. The protocol's appearance on memory consumption and a critical security metric are theoretically deducted through a probability model, and the resulting equations, with certain adjustment for real application, are guide by the simulations. In conformity with our evaluation, the comprehensive simulation results show that the DHT-based protocol can identify node clone with high confidence level and holds powerful protection in opposition to against adversary's attacks. Distributed Hash Table is a decentralized distributed system which provides a key based look up service. (Key,

record) pairs are stored in the table any active node can store and retrieve records associated with specific keys. Thus distributed hash table maintain mapping from keys to records among nodes. Chord is used and choose chord as a distributed hash table implementation to demonstrate protocol. Massive virtual ring is formed by chord in which every node is stay at one point, and owning a section of the periphery. Hash function is used to achieve pseudo randomness on output by mapping an arbitrary input into a b-bit space (in the ring).Chord coordinate is assigned for each node and can join the network. Here a node's Chord point's coordinate is the hash value of the node's MAC address [1].one segment that ends at the node's Chord point is related to every node, and all records whose keys fall into that segment will be transmitted to and stored in that node[5].Every node maintains a finger table of size t= O (log n) to further a binary-tree search. The finger table for a node with responsible for holding the t keys between 10 and 20.



- Figure 2. System architecture.

TABLE I: Distributed Detection Protoc --Ols Comparison, Where N Is Network Size, D Node Degree

Protocols	Nodes requirements	Communication cost	Memory cost	Detection Cost
Node to network broadcasting	Neighbors information	O (n)	O(d)	Strong
Randomized multicast	All nodes data	O (n)	O(d√n)	Acceptable
Line selected	All nodes data	O (√n)	O(d√n)	Acceptable
RED	Knowledge of network geography	O (√n)	O(d√n)	Strong
DHT	DHT nodes information	O (log n √n)	O(d)	Strong
RDE	Neighbors information	O (√n)	O(d)	Good

The DHT permit sensor nodes to build-up a chord overlay network. Cloned node may not join in this overlay network construction [1]. And this overlay network construction is independent of node clone detection. Nodes possess the information of their direct predecessor and successor in the Chord ring and also caches information of its consecutive successors in its successors table[6]. The communication cost is thus reduced by this cache mechanism and it enhances systems robustness. Selection of inspectors is done using the facility of the successors table.

Detecting Rounding Stages :

(i)The initial stage of detection round is done by activating all nodes by releasing an action message by initiator MACT=nonce, seed, time, {nonce||seed||time} k-1initiator During each rounds the value of nonce increases monotonously and it intended to prevent the DoS attacks.

ii)By receiving the action message each node verifies the value of nonce with previous values and verifies the signature of the message. If both are valid node will updates the nonce and stores the seed. The node perform observer to generate claiming information for each neighbor at the designated action time and transmits the message through the overlay network with respect to the claiming probability pc. Mα4β=idβ, Lβ, idα, Lα, { idβ ||Lβ ||idα ||Lα||nonce} k-1α. where, Lα, Lβ, are locations of α and β , respectively.

iii)Chord intermediate nodes will forwards claiming message to its destination node. Only the source node, Chord intermediate nodes, and the destination node need to process a message, whereas other nodes along the path simply route the message to temporary targets. Algorithm 1 for handling a message and If the algorithm returns NIL, then the message has arrived at its destination. Else the message will forwarded to the next node with the ID that is returned by Algorithm[1].

Algorithm 1:
dht handle message(Mα4β) handle a message in the DHT-based detection, where y is the current node's Chord coordinate, finger[i] is the first node on the ring that succeeds key((y+2b-I mod 2b),I £ [1,t] ,successors [j] is the next jth successor j £[1,g][1].
1: key<=H (seed||idβ)
2: if key £ [predecessor] then {has reached destination}
3: inspect Mα4β {act as an inspector, see Algorithm 2}
4: return NIL
5: for i=1 to g do
6: if key £(y, successors [i]) then {destination is in the next Chord hop}
7: inspect Mα4β {act as an inspector, see Algorithm 2}
8: return successors [i]
9: for j= 1 to t do {for normal DHT routing process}
10: if key £ [(y+2b-I mod 2b, y)], then
11: return finger [j]
12: return successor [g]

Message for node clone detection is examined by Algorithm 1 and Algorithm 2 compares the message with previous inspected messages that are buffered in the cache table[1]. All records in the cache table should have different examinee ID. If there exist two messages Mα4β and Mα'4β' satisfying idβ = idβ' and Lβ ≠Lβ shows that exists clone and then the witness node broadcasts the evidence to notify the whole network. All integrity nodes check the evidence information and stop communicating with the duplicate nodes. The witness does not need to sign the evidence information.

B. RANDOMLY DIRECTED EXPLOR -ATION (RDE):

This is designed to produce highly efficient communication appearance with satisfactory detection probability for dense sensor networks. In the protocol, initially nodes send claiming messages containing a neighbor-list along with a maximum hop limit to randomly selected neighbors; then, the subsequent message transmission is regulated by a Probabilistic directed technique to relatively maintain a line property through the network as well as to incur sufficient randomness for better Performance on communication and resilience against adversary. In addition, border determination mechanism is employed to further reduce communication payload. During forwarding, intermediate nodes explore claiming messages for node clone detection. By design, this protocol consumes almost minimal memory, and the simulations show that it outperforms all other detection protocols in terms of communication cost, while the detection probability is satisfactory.

Initially the node duplication detection is activated by the initiator. At the right mentioned action time, each node produce its own neighbor list (ID of neighbor and location). Then that node act as an observer for all its neighbors and starts to generate claiming messages. The claiming message involves node ID, location and its neighbor list[6]. The claiming information by node is created by Mα=ttl, idα, Lα, neighbor list where ttl is time to live.

The problems associated with the dht are it incurs more communication cost because of the hard overlay network and thus it is sensitive to energy and storage consumption. To overcome these problems a new node clone detection protocol introduced namely RDE(randomly directed exploration). Here the each node only needs to know and buffer a neighbor list having all neighbors ID and locations. During detection round each node constructs claiming message with signed version of neighbor list and then deliver message to others which will compares with its own neighbor list to detect node clone. If there exists any node clone, one witness node successfully catches the clone and notifies the entire network by broadcasting. The way to achieve RDE needs some techniques and routing protocols. First the claiming message needs to provide maximum no of hops and it is sent to random neighbors. Then the further message transmission will maintain a line and this transmission line property enables a message to go through a network as fast as possible[6]. The communication cost of this protocol is less and it is limited by the border determination mechanism. And the assumption made here is that each node knows about its neighbors locations.

Algorithm 2: RDE-process message Mα: An intermediate node processes a message
1: verify the signature of Mα
2: compare its own neighbor list with the neighbor-list in Mα
3: if found clone then
4: broadcast the evidence;
5: ttl<=ttl-1 6: if ttl ≤ 0 then

7: discard Mα
8: else
9: next node<=get next node (Mα) {See Algorithm 4}
10: if next node =NIL then
11: discard Mα
12: else
13: forward Mα to next node[6]

PERFORMANCE ANALYSIS

For the DHT-based detection protocol, the succeeding exact measurements are used to calculate its performance: Average number of transmitted information, representing the protocol's communication cost; Average size of node cache tables, standing for the protocol's storage consumption; Average number of witnesses, serving as the protocol's confidence level for the reason that the detection protocol is deterministic and symmetric.

III. ERCD Protocol

Initially, network region is nearly divided into h adjacent rings, where every ring contains a sufficiently sizable amount of sensor nodes to forward on the ring and also the breadth of every ring is r. To alter the outline, we tend to use hop length to represent the smallest number of hops within the paper. Since we tend to think about a densely deployed WSN, hop length of the net-work is that the quotient of the space from the sink to the sensor at the border of network region over the transmission vary of every sensor, i.e., the space of every hop refers to the transmission vary of sensor nodes. The ERCD protocol starts with a breadth-first search by the sink node to initiate the ring index, and every one neighboring sensors periodically exchange the relative location and ID data. Thus, whenever a sensor node establishes a data transmission to others, it has to run the ERCD protocol, i.e., witness selection and legitimacy verification, to verify its legitimacy. In witness selection, a ring index is randomly selected by the mapping function as the witness ring of node a. To help relieve the traffic load in hot spot, the area around the sink cannot be selected by the mapping function. After that, node a sends its private information to the node located in witness ring, and then the node forward the information along the witness ring to form a ring structure. In the legitimacy verification, a verification message of the source node is forwarded to its wit-nesses. The ring index of node , denoted Oa, is compared with its witness ring index to determine the next forwarding node. If $Oa\omega$> Oa , the message will be forwarded to any node located in ring Oa+1 ; otherwise, the message will be forwarded to any node in ring Oa -1. This step can forward the message toward the witness ring of node a. The ERCD protocol repeats above operations until a node, denoted b, located in the witness ring $Oa\omega$ is reached. Node b stores the private information of node a and forwards the message to any node located in ring $Oa\omega$ within its transmission range, denoted asc. Then, node c stores the information and forwards the message to the noded, where link (c,d) has longest projection on the extension line of the directional link formbook. The procedure will be repeated until node b reappears in the transmission range. Therefore, the witnesses of node a have a ring structure, consisting of b; c;…b In the legitimacy verification, node a sends a verification message including its private information following the same path towards the witness ring as in witness selection. To enhance the probability that witnesses can successfully receive the verification message for clone detection, themes-sage will be broadcast when it is very close to the witness ring, namely three-ring broadcasts, i.e., the message will be broadcast in $Oa\omega - 1$,$Oa\omega and Oa\omega + 1$ .we prove that the three-ring broadcasts can ensure the network security, i.e., the clone detection probability is one, under the assumption that all witnesses are trustful. To determine whether there exists a clone attack or not, all the verification messages received by witnesses are forwarded to the witness header along the same route in witness selection. The sensor nodes in the transmission route but not located in the witness ring are called the transmitters. The witness header of the source node a, denoted by Sa and is a sensor located in witness ring Oa meanwhile it is also in the communication range of the transmitter located in ring index $Oa\omega - 1\ or Oa\omega + 1$. The witness header Sa is randomly selected by the transmitter in the neighboring witness ring, i.e., the ring of $Oa\omega - 1\ or Oa\omega$ +1 . If more than one copie or incorrect copies or expired copies are received by the witness header, the ERCD protocol will generate a cancellation procedure; if no copy is received from the source node due to packet loss or silent cloned node, transmissions from the source node will not be permitted. The verification messages of both a and a0 are broadcast in ring $Oa\omega - 1, dOa\omega + 1$ after that, both messages are received by the witness header Sa, and a revocation procedure is triggered. We describe the detail of the ERCD protocol in Algorithm. In addition to the normal operations, the recovery mechanism is very easy to be established based on ERCD protocol. For the case when the clone detection fails due to interruption or clone attack, another clone detection cycle will be initiated and the origin node will randomly choose a new route and transmit the message enroot to a new witness header.

Probability of clone detection: In distributed clone detection protocol with random witness selection, the clone detection probability generally refers to whether witnesses can successfully receive the authentication message from the source node or not. Thus, the clone detection probability of ERCD protocol is the probability that the verification message can be successfully transmitted from the source node to its witnesses. In ERCD protocol, the verification message is broadcast when it is near the witness ring, i.e., in the rings of $Oa\omega - 1$,O$a\omega$&$Oa\omega$ +1, to guarantee the network security. With such kind of method and assumption of trustful witnesses, we can prove that at least one of the witnesses can receive the message, i.e., the clone attack can be detected with probability one. To simplify the analysis, the transmission ranges of all sensor nodes, are the same.
Algorithm: Energy and memory efficient clone detection protocol:

Phase 1
Step 1: Create a group of sensor nodes. The base station gives the different unique ID to each node and makes that node as original node.
Step 2: We divide a complete network into clusters.
Step 3: cluster head is selected in each cluster.

Phase 2
This phase-2 is applied for each separate cluster. ERCD algorithm is applied for over all distributed network, so there is a delay in detecting the clone attack is more. In this paper we apply algorithm for different cluster group so the delay in detection of clone attack will get reduced. We can see that delay result. The concept of ERCD algorithm is used for fair comparison.
Step 4: A random value is distributed by using centralized mechanism like satellite or any other central stations.
Step 5: Each node board cast its ID and location to its claim.
Step 6: Neighbors receive the broadcast and each neighbors sends the claim.
Step 7: The claim is send to any of the location. This is selected using pseudo random function. (We are not using any ID to select the location). Step 8: Before broadcasting, every node signs its message with its private key.
Step 9: Signature is verified at the destination end. At the destination ends: 1. The signature check is carried out by verifying the received signature.
2. Message freshness: The ID and location information is extracted from received message. At the destination end it simply stores the ID and location if the claim node is first carrying that ID and location. If it receives the same ID and location for second time, it checks for the coherence for ID and location. This is the proof of detection of clone with two in-coherent claims.
Step 10: The incoherent ID and location is checked with cluster head and also with base station. It detects the clone node.
Step 11: clone node information is broadcasted to all other nodes. By this we can avoid the claim of the clone node with other nodes in the network.

IV. Conclusion

Thus after identifying the weaknesses of proposed methods which has been done previously we proposed an efficient algorithm that covers various issues related to it. Using proposed algorithm it is possible to minimize the overhead of data packets. We have proposed distributed energy-efficient clone detection protocol with random witness selection. Specifically, we have proposed ERCD protocol, which includes the witness selection and legitimacy verification stages. Both of our theoretical analysis and simulation results have demonstrated that our protocol can detect the Clone attack with almost probability 1, since the witnesses of each sensor node is distributed in a ring structure which makes it easy be achieved by verification message. In addition, our can achieve better network lifetime and total energy protocol consumption with reasonable storage capacity of data buffer. This is because we take advantage of the location information by distributing the traffic load all overWSNs, such that the energy consumption and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended. In our future work, we will consider different mobility patterns under various network scenarios and improve the connectivity in sparse network number of mobile sink could be increased. Simulations can be extended with multiple mobile sink to cover the other parameters and scenarios such as fault tolerance, throughput and impact of data aggregation etc. Link failure due to the mobility of sink and node failure could also be taken into consideration for maintaining the reliable path.

References

[1]. Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: An energy-efficient clone detection protocol in WSNs," in Proc. IEEE INFOCOM, Apr. 14-19, 2013, pp. 2436–2444.

[2]. R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emergingmachine to machine communications," IEEE Commun.Mag., vol. 49, no. 4, pp. 28– 35, Apr. 2011.

[3]. A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," Comput. Netw., vol. 56, no. 7, pp. 1951–1967, May. 2012.

[4]. T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[5]. P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 7,pp. 1036–1045, Sep. 2010.

[6]. R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012.

[7]. Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," IEEE Netw., vol. 25, no. 5, pp. 50–55, May. 2011.

[8]. R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacypreserving key management scheme for location based services in VANETs," IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127–139, Jan. 2012.

[9]. H. Choi, S. Zhu, and T.F. La Porta, "SET: Detecting Node Clonesin Sensor Networks," Proc. Int'l Conf. Security and Privacy in Comm.Networks and the Workshops (SecureComm '07), pp. 341-350, 2007.

[10]. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. 9th ACM Conf. Comput. Commun. Security, Washington, DC, 2002, pp. 41–47.

[11]. Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks,"IEEE J. Sel. Areas Commun., vol. 28, no. 28, pp. 677–691, Jun. 2010.

[12]. B. Parno, A. Perrig, and V. Gligor, "Distributed detection of nodereplication attacks in sensor networks," in Proc. IEEE Symp. Secu-rity Privacy, Oakland, CA, USA, May. 8-11, 2005, pp. 49–63.

[13]. B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in largescale sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

*Garikapati.Divya . "On The Node Clone Detection Using Hashing In WSN." IOSR Journal of Computer Engineering (IOSR-JCE) 19.4 (2017): 68-73.