Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 9, September-2017

Energy Efficient Star Based Distributed Clone Detection in Wireless Ad-Hoc Network

Miss. Jigishaa Mahesh Bute

Flora Institute of Technology, Department of Computer Engineering, Pune, India

Abstract *--- Wireless Ad-hoc Networks are susceptible to clone attacks or node replication attacks because they are deployed in hostile and unattended environments where they are deprived of physical protection, needed physical tamper-resistance of sensor nodes. Consequently, an attacker can simply capture and compromise sensor nodes after replicating them, he inserts arbitrary amount of clones/replicas into the network. If these clones are certainly not simply detected, an opponent might be further competent to mount lots of internal attacks which may emasculate various protocols and device applications. Certain solutions happen to be proposed inside the literature to address the problem of clone detection that is not satisfactory as they are afflicted by some serious drawbacks. With this paper we advise an Energy-Efficient Distributed Star Based Clone Detection (ESCD) protocol which includes observer selection for verification stage. Our protocol may also achieve better efficiency as well as it will become trustful system.*

Keywords *--- Wireless Ad-hoc Networks, Clone Detection Protocol, Energy Efficiency, Network Lifetime.*

I. INTRODUCTION

Wireless Network could be an assortment of sensing element nodes with powerful sensing capabilities however restricted resources. They include advanced network architectures and therefore square measure employed in a good sort of applications. These sensors lack tamper resistance hardware thanks to price issues and square measure typically deployed in robust and rough settings and vicinities, hostile situations and unnoticed standing. Thus, they offend the fraud from the offender and malefactor which might launch several attacks together with the intention to accumulate essential info from the WSN or to disable and exhaust the tasks of the WSNs. Here, we tend to particularly specialize in a lot of harmful attack that is understood as node replication attack or clone attack. During this attack a person well captures one or a lot of sensing element nodes and understanding all its secret authorization. The node compromise consequently permits AN person to be capable of making clones or replicas of the compromised nodes and then secretly deploying them at essential positions of the network.

An important distinctive behavior of clones or replicas is that they act as legitimate nodes or recognized participants within the network. These clones settle for the cryptanalytic keying materials which permit them to appear like original legitimate sensing element nodes. Since, they behave fairly and perform within the network operations like non-compromised sensing element nodes so the legitimate and honest nodes aren't conscious of that there's a clone node

among them. Consequently, all the present authentication techniques and secure network communication protocols would simply permit these replicas to make try wise shared keys with different node and also the base station, conjointly permissive them to encrypt/decrypt all their communications. If these clones aren't disclosed certainly, fleetly and promptly, a person will simply head of the network by exploiting these clones. Moreover, he/she will cripple several applications of the Wireless Ad-hoc Network because it is extremely straightforward for him/her to compromise and replicate a typical sensing element node by employing a few pronto out there tools in a very short amount of your time. Also, once a person captures and compromises one sensing element node, it becomes the bottom to form clones and therefore the most price of attack is management. An offender may weight these clones for dispatch several business executive attacks and malicious activities. for instance, he/she will produce a region, initiate a hollow attack once many clones group along, launch selective promote attack and DOS attack, inject false knowledge, monitor and catch good portion of traffic, denigrate and offend different nodes and even terminate legitimate nodes.

The most straightforward but unassertive solution to handle these clone node attacks is to equip the sensor nodes having a tamper resistant hardware however this option would be incorrect because of two main reasons first, it really is costly and extremely costly to shield all the sensor nodes inside the network having a tamper proof hardware, and second, it may static be easy to neglect tamper protection with an expert attacker. So, there's a must develop software based countermeasures for your detection of clone nodes. Within the article two kinds of software based solutions are already proposed for your detection of clone attack in static WSNs namely Centralized and Distributed.

II. LITERATURE REVIEW

2.1 Paper Name: ERCD: An Energy-efficient Clone Detection Protocol in WSNs [1]

Authors: Zhongming Zheng, Anfeng Liu , Lin X. Cai , Zhigang Chen , and Xuemin (Sherman) Shen

Description: A location-aware clone detection protocol, which guarantees sure-fire clone attack detection and has very little negative impact on the network time period. Specifically, we tend to promote the placement info of sensors and at random choose witness nodes settled in a very ring space to verify the privacy of sensors and to notice clone attacks. The ring structure facilitate energy economical knowledge forwarding on the trail towards observe and therefore the decline and therefore the traffic load is distributed across the network, that improves the network time period somewhat. Theoretical analysis and duplicate results demonstrate that the planned protocol will approach 100% clone detection likelihood with confiding witnesses. we tend to any extend the work by study the clone detection work with un-trustful witnesses and show that the clone detection likelihood still approaches ninety eight once 100% of witnesses square measure compromised. Moreover, our planned protocol will somewhat improve the network time period, connected with the prevailing approach.

Advantage: Location-aware clone detection protocol for clone attack detection

Limitation: Attacker uses the replica node to insert fake data and disturb the whole operations in the network.

2.2 Paper Name: Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive [2]

Authors: Routes Tao Shu, Sisi Liu, and Marwan Krunz

Description: In this paper, we tend to study routing system that bypass black holes found by these attacks. We tend to argue that existing multi-path routing approaches are prone to such attacks, principally because of their settled

description. Thus once wrongdoer achieves the routing formula, it will work out identical routes well-known to the supply, and therefore endanger all info sent by these routes. During this paper, we tend to develop structure that develops irregular multipath routes. Underneath our style, the routes taken by the shares of specific packets modification over time. Thus notwithstanding the routing formula becomes well-known to the wrongdoer, the attackers still cannot pinpoint the routes leave out by every packet. Besides volatility, the routes generated by our mechanisms are extremely dispersive and energy-efficient, creating those quite capable of omit black holes at low energy price. Large simulations are conducted to verify the validity of our mechanisms.

Advantage: Generate randomized multipath routes.
Limitation: Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs).

2.3 Paper Name: Distributed Detection of Node Replication Attacks in Sensor Networks [3]
Authors: Bryan Parno, Adrian Perrig, Virgil Gligor
Description: During this paper authors proposed two new algorithms supported resulting properties, i.e., properties that collect solely over the collective action of multiple nodes. Irregular Multicast issue node location data to arbitrarily elite observer, exploiting the birthday ambiguity to discover replicated nodes, whereas Line-Selected Multicast uses the topology of the network to discover replication. Every algorithm organizes globally-alive, distributed node-replica detection, and Line-Selected Multicast illustrations pointedly strong performance characteristics. We tend to show that showing algorithms represent a bright new approach to detector network security; likewise, our results naturally be different categories of networks within which nodes are often captured, replicated associated re-inserted by an mortal.

Advantage: To detect replicated nodes.
Limitation: Node replication detection schemes depend primarily on centralized mechanisms with single points of failure.

2.4 Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks [4]
Authors: Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo and Li Xie
Description: In this paper they propose two new NDFD protocols, Random Walk (RAWL) and Table-assisted Random Walk (TRAWL), which fulfill the requirements while having only prepare communication and memory upward. Our simulation results show that our protocols exceed an existing NDFD protocol with the lowest overheads in witness selection, and TRAWL even has lower memory overhead than that protocol. The communication overheads of our protocols are higher but are fair considering their security benefits.

Advantages: Randomized Multicast is NDFD and fulfills the requirements of clone detection.
Limitation: It has very high communication overhead.

III. PROPOSED SYSTEM

1. In this we proposed a system that besides the clone detection possibility, we also consider energy consumption and memory storage in the design of clone detection protocol, i.e., an energy and memory-efficient distributed clone detection protocol with random witness selection scheme in wireless ad-hoc networks.
2. Our protocol is applicable to general densely deployed multi-hop wireless networks, where adversaries may compromise and clone sensor nodes to launch attacks.
3. We extend the analytical model by evaluating the required data buffer of ESCD protocol and by including experimental results to support our theoretical analysis. Energy-Efficient Distributed Star Based Clone Detection (ESCD) protocol.
4. We find that the ESCD protocol can balance the energy consumption of sensors at different locations by distributing the witnesses all over wireless networks except non-witness distributed stars, i.e., the adjacent distributed stars around the sink, which should not have witnesses.
5. After that, we obtain the optimal number of non-witness distributed stars based on the function of energy consumption.
6. Finally, we derive the expression of the required data buffer by using ESCD protocol, and show that our proposed protocol is scalable because the required buffer storage is dependent on the distributed star size only.

3.1 Advantages of Proposed System:

1. The performance of the ESCD protocol is evaluated in terms of clone detection probability, power consumption, network lifetime, and data buffer capacity.
2. Extensive simulation results demonstrate that our proposed ESCD protocol can achieve superior performance in terms of the clone detection probability and network lifetime with reasonable data buffer capacity.
3. The experiment results demonstrate that the clone detection probability can closely approach 100 percent with untruthful witnesses.
4. By using ESCD protocol, energy consumption of sensors close to the sink has lower traffic of witness selection and legitimacy verification, which helps to balance the uneven energy consumption of data collection.

3.2 Applications of Proposed System:

1. Cyber physical network system.
2. In any Real time wireless sensor network.

IV. SYSTEM ARCHITETURE

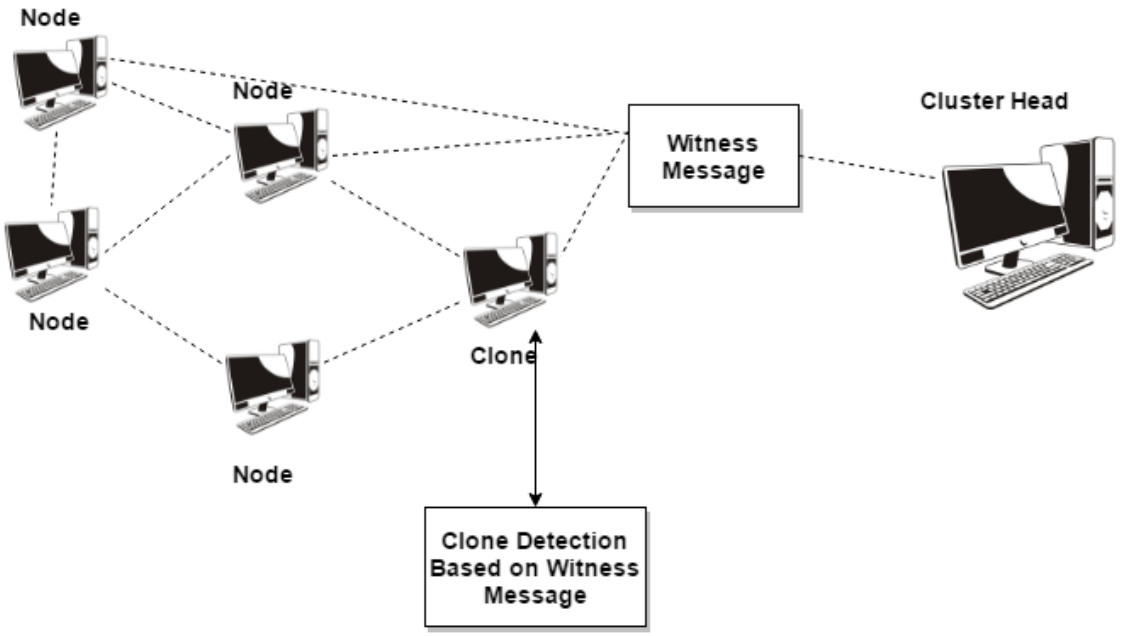

Figure 4.1 System Architecture of Proposed System

In the proposed system, each node from the network will be assigned an original certificate by the cluster head during the time of node initialization the certificate will be utilized for witness message at the time of clone detection within the cluster. The device is designed in the distributed star topology where each node is coupled to the cluster head separately which causes the less energy and storage needed for each node as well as for cluster head while detecting the clone. The cluster head sends get each node in the cluster for witness message, depending on the witness message the cluster head will detect the clone as the witness message is not nevertheless the certificate given by the cluster head for each node.

V. MATHEMATICAL MODEL

Let S be the whole System:

S= {N, CH, W, C}

Where,

1. N is the number of nodes.

N= {n1, n2, n3….. n}

2. CH be the Cluster head

CH= {ch1}

3. W be the Witness messages

W= {w1, w2….. wn}

4. C be the Clone nodes

C= {c1, c2, c3…..cn}

Step 1: Node N will login into the system through ID and Password.

Step 2: After Login system S will authenticate the node.

Step 3: The Node will send the file to the database. When Node is sending file to database then at that time another node i.e. Clone node will also send the file.

Step 4: After receiving the files from Node and Clone node the system is requesting for Witness message.

Step 5: If the node will able to send the witness message then it is a valid node otherwise the clone is detected.

VI. RESULT ANALYSIS

Here, Whole System has taken many attributes for the input purpose but here author mainly focuses on the accuracy, time, storage and energy cost of system. Based on this attributes we are getting following analytical result for our proposed system with respect to existing system.

Expected Result

	Existing	Proposed
Accuracy	8	10
Storage	10	2
Energy	8	4
Time	10	6

Where,

A = Privacy and security.

B = Computation Cost/ time.

C = Accuracy

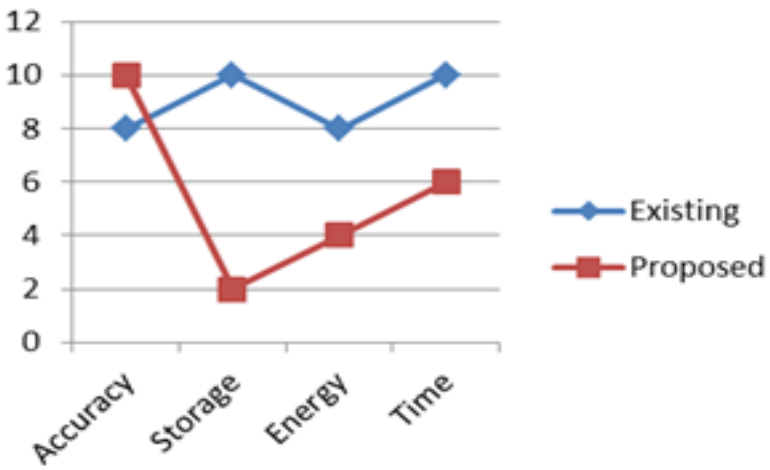

Figure 4.2 Existing System vs. Proposed System Graph

VII. CONCLUSION

In this paper we proposed distributed power efficient clone detection protocol with random witness selection. Specifically, we now have proposed the ESCD protocol, such as the witness selection and legitimacy verification stages. Also, our procedure is capable of doing improved network lifetime and overall energy consumption with reasonable storage capacity of data buffer. The vitality consumption and memory storage in the sensor nodes round the sink node could be relieved along with the network lifetime could be extended.

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, Turin, IT, Apr. 14-19 2013, pp. 24362444.

[2] T. Shu, M. Krunz, and S. Liu, Secure data collection in wireless sensor networks using randomized dispersive routes, IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941954, Jul. 2010.

[3] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, Distributed detection of clone attacks in wireless sensor networks, IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685698, Sep. - Oct. 2011.

[4] B. Parno, A. Perrig, and V. Gligor, Distributed detection of node replication attacks in sensor networks, in Proc. IEEE Symposium on Security and Privacy, Oakland, CA, USA, May. 8-11 2005, pp. 4963.

[5] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, Random-walk based approach to detect clone attacks in wireless sensor networks, IEEE Journal on Selected Areas in Communications, vol. 28, no. 28, pp. 677691, Jun. 2010.

[6] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 127–139, Jan. 2012.

[7] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.

[8] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symposium on Security and Privacy, Oakland, CA, USA, May. 8-11 2005, pp. 49–63.