iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3232

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

A Detailed Discussion on Node Replication Attacks in Static WSN

Mrs. N.S. Usha[1], P. Anandhaa Lakshmi[2], S. Jeevitha[3]
[1]*Associate Professor,* [2, 3]*Department of Computer Science And Engineering, S.A. Engineering College*

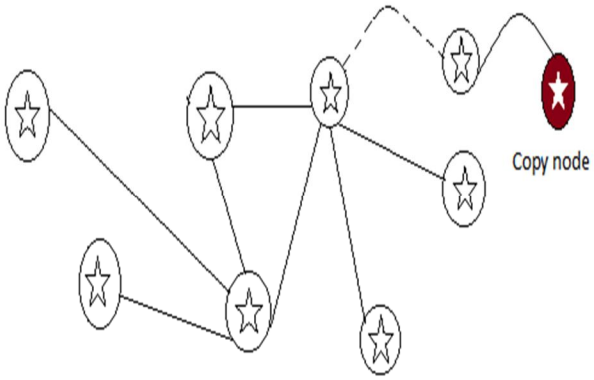
Abstract: ***Wireless sensor nodes gather sensory information from connected nodes that are processed to get relevant results are prone to clone node attacks such as wormhole, sinkhole, eavesdropping and DOS attack where several measures like SET, location aided, witness based detection have been brought to detect them. Clone node attack is one in which the attacker fetch a node from a network and makes a replica to take control over the network. If the attack is not detected then the replica consumes the resource and makes the network vulnerable to large internal attacks. In this literature abundant number of schemes in proposed systems is provided in general that achieves good communication performance, high detection probability, and energy efficiency. But it fails to provide security, effective cost, efficient storage, and accuracy.***

I. INTRODUCTION

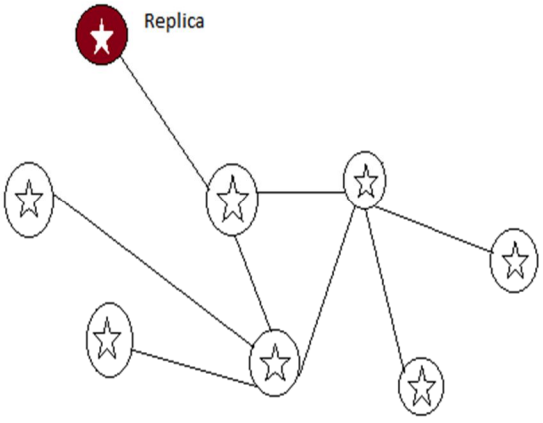
Wireless sensor network refers to a group of self-sufficient nodes with sensing capabilities. A heavily deployed node can communicate with each other and performs simple operations with constrained power. Wireless sensors have been employed widely over a variety of applications ranging from monitoring environment to tracking objects. The sensors are prone to various attacks. For example, The attacker compromises the information of some sensors within the network and gather their private information. Then, the sensors are cloned and are deployed in Wireless sensor networks and these are susceptible to a variety of attacks known as clone attack. The cloned nodes contain the same information such as code and cryptographic information; they take part in the network operations and initiate the attack. The cloned node attacks have become a serious critical issue. So it becomes vital to detect these clone attacks. For the clone, detection Witness is selected. They are randomly selected and at least one witness node receives the authenticated messages for detection. The Witness verifies the identity of nodes to check if they are prone to attacks or not. The sensors are small in size, with limited battery power and memory efficiency.

Sensors must not only provide high performance, but they must also be memory efficient. Some clone detection protocols have been proposed such as Randomized Efficient and Distributed protocol (RED) and Line-Select Multi-cast protocol (LSM). But, many approaches focus to develop a clone detection mechanism without evaluating efficiency and memory consumption. Hence, to assure successful clone detection, the Witness must contain a record of all legal information of the source node. Thus, huge memory is required to record all the information of sensors. so, it becomes tedious for densely-deployed WSN. Thus, sensors of low cost with efficient power and memory efficiency must be deployed. In most cases, they are prone to single point failures, where the base station that contains all the information of nodes fails. If the base station fails, then it leads to the degradation of performance of nodes.

Static WSN



Static WSN With Replica



II. RELATED WORKS

The author yingpei and shingengzang [1] has proposed an NDFD (Non-Deterministic and Fully Distributed) protocol such as RAWL (Random Walk) and TRAWL (Table Assisted Random Walk). During node attacks, an adversary compromises a few nodes and replicates them. Later it inserts the arbitrary number of replicas into the network. They achieve moderate memory overhead. It is vulnerable to simple witness compromising attacks and also has high communication overhead. Shriya autkar [2] shows a node in a centralized approach sends an ID, neighbor list as a message to claim it from the base station. Replicas are detected in the network by flooding the neighbor list with authenticated revocation messages. The base station examines the list, if two nodes are identified with the same id then one of a node is found to be a clone.

WibadaNaureuphipat, Yung Ji, chalermpolchamsripinyo [3] stated that area based approach can be used to distinguish between good nodes and malicious nodes. This approach detects the attacker when he acts as an intermediate node. Achieves high successful detection rate while decreasing communication overhead. It can also maintain network lifetime and decreases the number of stored messages. They lack in computing, processing power, and energy supply.

[4] Zhijunli, Guang gong uses Distributed Hash Table (DHT) which is a decentralized technology. DHT uses key-based caching which identifies the replica effectively. The second approach which is implemented was randomly directed exploration. The main pros of this paper are good communication performance and border detection. Even though communication is good, the setup cost is high. [5] Balmukund Mishra proposed a centralized scheme that uses efficient protocols like RED (randomized efficient and distributed) & LSM (Low Selected multicast). The major attacks happening here are eavesdropping, DOS, energy depletion and capturing attack. Disadvantages of this paper are heavy traffic and lifetime of this node is reduced. [6] Kai Xing has proposed a best scheme detecting clone attack. By using neighborhood properties a social fingerprint is computed. With help of generated social fingerprint, it identifies the legitimate user. This method has high detection accuracy but it restricts the memory for resources. Zhihua Zhang, ShoushanLuo, Hongliang Zhu, Yang Xin [7] used witness based location dependent algorithm and are similar to LSM, RED, LSCD, protocols. It has a higher detection probability equal to 1. They have compared to ERCD and LSCD it has low resource expenditure and a longer lifetime. It has a high detection probability and makes full use of energy nodes in the non-hotspot area.

Nadhiya.N, prashanth.C.R [8] stated that the mechanism consists of a set of sensor nodes from a network called the witness, using which it proves the legitimacy of nodes. So, if any sensor node wants to transmit data, it sends a request to witness. Through this, the private information is being shared. It uses randomly selected witnesses and at least one of the witness nodes can successfully receive all verification messages. Hemavathy.Y, Keerthiga.M, Jeyamohan.H [9] used two novel node clone detection protocols. They are based on DHT and are based on distributed detection protocol. It is easy and cheaper to implement. Every node needs the neighbor list of all neighbor, ID, and location. It implements the RDE protocol. Every region has a group leader who generates a random number with a timestamp to available nodes. The messages are encrypted in this mechanism.

P.S.mann [10] uses centralized techniques and SET. It involves security attacks like Sinkhole attack, Wormhole attack, and Sybil attack. The single hop detection uses fingerprint verification phases. After the two nodes encounter with each other, they interchange node list and if there is a conflict it implies replica of one node. The security requirements are availability, authorization, authentication, confidentiality. K.Ravikumar, V. Manikandan [11] considered the network to be a set of non-overlapping sub-counties. An exclusive subset is formed in each sub-region, if the connection of subset is not empty it implies that replicas are included. It involves three phases namely, Key distribution, Shared key and path key Establishment. The nodes share secret keys between two nodes which are given by Modified Bloom's Scheme (MBS).

Irfan Khan [12] in his clone detection mechanism used ERCD protocols to achieve high detection probability. It includes two stages namely, Witness selection and legitimacy verification. The witness selection uses random mapping function and the Legitimacy verification verifies the request sent from source to witness which contains privacy of source nodes. The witness is usually ring structured which makes it easy to achieve verification messages. SachinLalar, ShashiBhushan, Surendra [13] stated that the clone node attack creates depth damage to the community and corrupts monitoring system. In the centralized method, if the base station fails then the clone node detection also fails. In this method, the node ID is exchanged among neighboring nodes. It uses a straight forward scheme where a new node wants to join the network it publicizes message with ID and location to the neighbors.

Roshani Tamale, RupikaYadav, Vishal Tiwari [14] stated that all the nodes send information to cluster head where aggregation of information occurs. It involves two types clustering namely Homogeneous and Heterogeneous clustering. In distributed clustering, each node maintains own algorithmic rules whereas in centralized, the authority teams nodes to make clusters. It uses ERCD protocol which upon receipt of routing information updates routing table. N.S.usha, P.SrilekhaNivetha [15] classifies WSN as SWSN (Static Wireless Sensor Networks) and MWSN (Mobile Wireless Sensor Networks). They are prone to attacks such as Layer

dependent and layer independent attacks. Layer-dependent attacks include routing attack and layer independent attacks include Sybil attack.It involves the creation of many replicas with the same ID. They use message encryption and authentication mechanisms. Selvi, P.shobana [16] used the base stations with a huge number of low- end sensors. The challenger may drop or manipulate reports. The lifetime of batteries are extended.They provided a solution for WSN attacks using robust cryptographic strategies.It improved LEACH protocol using location information of nodes In network

III. COMPARISON TABLE

Attacks	Principles	DE-MERITS	Network Architecture	Security
Denial of service(DOS) attack	All purpose	Capacity is reduced & requires large no of system	Traditional WSN	Interruption, Interception, Modification
Wormhole attack	To be authenticated & authorized	Leads to DOS, blackhole attacks	Traditional WSN	Fabrication, Interception
Replayed routing information	unfairness	Generates false error messages	Large and Traditional WSN	Fabrication
Collision	unfairness	Packets are discarded, Cost effective	Large & Traditional WSN	Modification
Resource exhaustion	unfairness	Compromise availability	Traditional WSN	Modification
Sybil attack	unfairness	Threat to routing, Expensive	Traditional WSN	Fabrication, Modification
Acknowledge spoofing	unfairness	Provides false information to neighboring nodes	Traditional WSN	Fabrication

IV. CONCLUSION

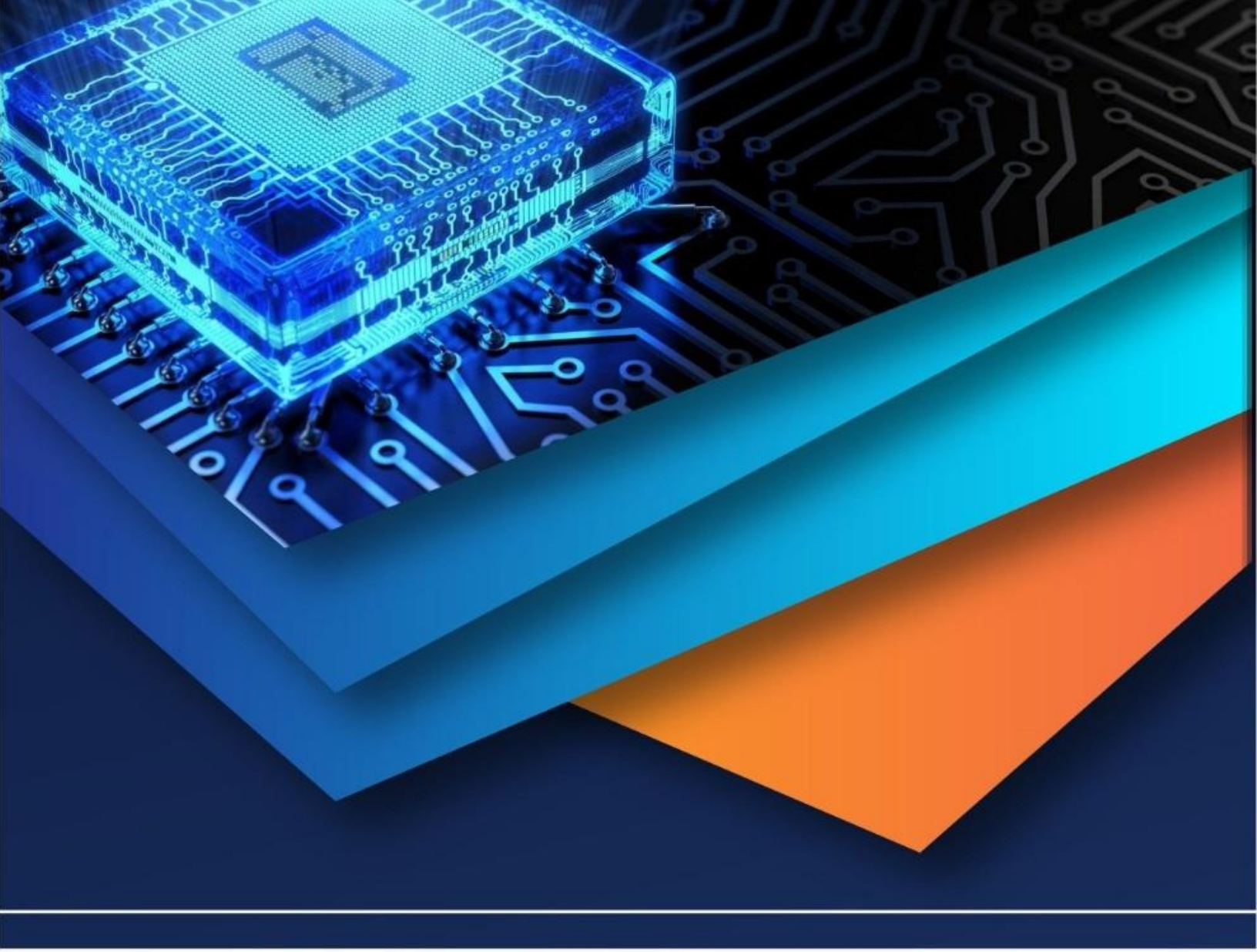
In this paper, we include memory efficiency and power consumption in clone detection. We proposed an idea of placing the nodes at equal distances i.e. implementation of Destination Sequence Distance Vector (DSDV) protocol. The distance between all the nodes in the network is the same. This is implemented by calculating the hop count of the nodes. Every time, the hop distance is recorded for each node. The cloned nodes are unaware of the hop count. So, during data exchange, we could easily detect them. Moreover, the replicated nodes could not place an exact location. Thus, it becomes easier to detect the cloned nodes. The hop count includes the transitional devices like routers through which data is transferred from source to its destination.

This is achieved using NS2 (Network Simulator) tools. It is an open source simulation tool which is targeted at networking research to support routing and IP protocols such as TCP, UDP, etc. Once, the hop count has deviated or if there occurs any change in the location of a node with respect to other nodes, thus the clone nodes are detected. It provides us with the simulated output. The nodes are employed in a grid architecture.

REFERENCES

[1] Yingpei, Jiang cao, shingengzang, shanquingguo (2010) IEEE journal on selected areas in communication. Random walk based approach to detect clone node in WSN.
[2] Shriya v. Autkar, M.R. Dhage, s .p. Bholane (2015) International conference on pervasive computing Distributed techniques.
[3] WibhadaNaureuphipat, Yung Ji, chalermpolchamsripinyo (2012) IEEE 11th International Conference on Trust, Security, and Privacy in Computing and Communication.An Area-based approach for clone node detection in WSN.
[4] Zhijunli, Guang Gong. (2012)IEEE/ASM transactions on networking on the node clone detection in WSN.
[5] Balmukund Mishra, Yashwant Singh (2015) Third international conference on ICIIP. The approach towards optimization of clone node attack.
[6] Kai Xing, Fang Liu, Xiuzhen Cheng, David .H .c .du. (2008) The 28th International conference on Distributed computing systems. Real-time detection of clone node in WSN

[7] Zhihua Zhang, ShoushanLuo, Hongliang Zhu, Yang Xin (2018). A clone detection Algorithm with low resource expenditure for WSN.
[8] Nadiya .N, Prashanth .C.R (2017) International journal of computer science & communication networks. Secured clone detection using witness head selection to avoid malicious nodes in WSN.
[9] Hemavathi .Y, Keerthiga .M, Jeyamohan .H (2017) International Journal of Latest engineering & Management Research. Clone detection using chord algorithm in WSN.
[10] P.S. Mann (2014) International Journal of Research in computer application & Robotics. Detection of clone attacks in WSN.
[11] k. Ravikumar, V. Manikandan (2018) International Journal on scientific research in computer science & engineering. Detection of node capture attacks in WSN.
[12] Irfan Khan (2018) International Journal for Technological Research. Find out clone detection mechanism techniques in WSN.
[13] SachinLalar, ShashiBhushan, Surrender (2017). Analysis of clone detection approaches in static WSN.
[14] Roshani Tamale, RupikaYadav, Vishal Tiwari (2017) International Journal on Recent & Innovation Trends in computing & communication. Clone detection for an efficient system in WSN using AODV.
[15] N.S. Usha, K. SrilekhaNivetha (2018) International Journal of Innovative research in science, Engineering & Technology. Identification of clone nodes in static WSN using a secured key Distributive Mechanism.
[16] T. Selvi, P. Shobana (2017) International Journal of Advanced Research in computer science. High efficient Approach clone attack detects using Digital WSN.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY