An Efficient Clone Node Detection Scheme using Enhanced Random walk in Wireless Sensor Network

K. Sindhukavi, P. Brundha, P.J. Beslin Pajila
Department of CSE with specialization in networks,Francis Xavier Engineering College, Vannarpettai, Tirunelveli-627003
***Corresponding author: E-Mail: sindhukavi22@gmail.com**

ABSTRACT

The network which is wireless and spatially arranged in an ad hoc manner is referred as Wireless sensor network. This sensor network prevent message replay via many techniques like authentication, cryptography, message integrity etc. In existing system WSNs worked with distributed hash table.

The familiar paths extend with unfamiliar nodes and set up a ring path on perpendicular direction for locating route of a DHT protocol. At the same time DHT is an effective challenger which is enhanced to the improvised version of Clone Detection via duplicate the node identities (IDs). To overcome this, Enhanced Random Walk (ERW) based clone node detection scheme overcome this problem by construct catch clone nodes through a checking system. The probability modeling in this technique theoretically avoids both critical security metric and protocol completion on memory consumption.

KEY WORDS: wireless sensor network security, clone detection protocol, Enhanced Random Walk.

1. INTRODUCTION

The WSN is the one of the ultimate design of the Cyber-Physical classification. The information exchanged in network get easily replaced in WSN's secure communication is it is vital in nature. So that an antagonist used for seizures the sensored node and collect all the information. Also the adversary can duplicate that's why a new network is developed for performing different malicious attacks. The above mentioned attack is technically referred as a cloned attack. The clone attacking and resource contained sensor node to alleviate node seizure are done via a new scheme called Witness-based clone detection. This method identifies forward nodes identities and coordinates and moves like a witness node. These techniques used the facts like the captured clone node has the same identity but this on the different locations. This time also the clone detected while the two nodes have the same identities and are stay in a different locations.

The accessing of legitimate information, the non-compromised manner operation of a nodes and arising of various attacks are the major problems caused by a cloned node. The DHT mainly consist the more service which is related to the hash table. It contains pairs of data like (key, value) and the data stored in DHT. DHT is a group of disperse shared system contains look up services. The disruption can be decreased via removing the group of active members on the basis of arranged node's value. Also the DHT scale the infinity of nodes and control continuous flow of nodes and their failures. This technique extends with the architecture Enhanced Random Walk (ERW). The specified nodes are identified the location claim and find out the errors randomly forwarded nodes. The irregular moments in network starts on the basis of when the randomly select exchanged information has any claim to report. The actively passing node is considered as a witness and also reports the claim.

Related Works: Liu (2015), has proposed a Logging joint marking scheme. The LM scheme not needs a maximum amount of storage capacity, minimum amount of storage enough to perform algorithm. But there is need to storage equality between the nodes. It is a satisfiable storage medium. This scheme provides a support in various ways for storage utilization. High overhead can occur due to this drawback this scheme was neglected.

Luo (2011), has invented a method is a Lightweight method. This method used to perform in clone node for detecting the various attacks. This scheme achieved by maximum detection of attackers and reduces the transmission cost of each node by taking advantage of temporal and spatial uniqueness in physical layer channel responses. This method helps to minimizing the packet transmission overhead. Due to low security, this technique was not popular.

Zeng (2010), A new RED protocol is invented for finding attacks used node replication .this technique is high efficient in communication. Due to low robustness among compromise attacks, this technique does not work perfectly.

Zhu (2012), Localized Multicast, one node is randomly picked up from the geographically limited region. Here all nodes are deployed. The selected node will be considered as witness node. This technique is increase the probability of detection ratio. The problem in a system is communication costs are critically high.

Sindhukavi (2016), has developed the advanced hash table algorithm, system uses Distributed Hash Table in WSNs. This protocol can makes a route path with horizontal direction of a known path with known nodes deployed in a ring path. It verifies the detection path because the witness path length is must be more than the detection path. The clone detection process is carried out in the no-hotspot region in LSCD protocol. Energy efficiency is very high in this existing mechanism but no assurance for secured transmission. That is why this system fails.

2. PROPOSED DETECTION SCHEME

Enhanced Radom Walk method is proposed for overcome a problem in Hash table detection protocol. In this each node transmits a signed location claim. The selected node gets a claim from the each neighbor node. Claim message used to start a random walk send by the chosen node. If any other node get a different location for a same node ID That node is indicated as replicated node.

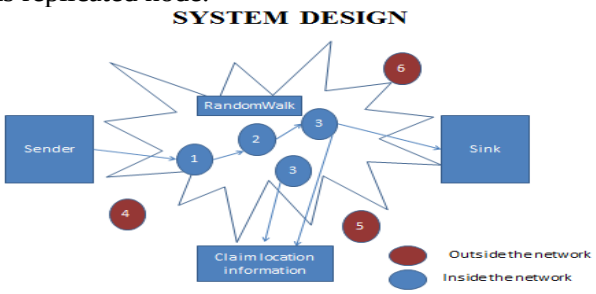

Figure.1. System Architecture

Fig.1, defined as data transformation from sender to sink. Nodes are placed in inner network and outer network. The sensor nodes are defined to know their relative locations. In relative location sensor nodes are defined. The sender sends a data to node and that particular node forward to nearby node. If two nodes have a same ID then it detect that node using Cloned detection protocol based on Enhanced Random Walk (ERW) and finally data reach the sink.

Network Model: 100 amounts of nodes could be deployed in the NS2 simulator. Which are in movable. The simulation will consider the parameters such as frequency, antenna type, routing protocol and security schemes.

- The source and destination nodes are declared
- The transmission path is calculated.

Detection of Clone Node by Random Walk Method: Broadcast authenticator scheme is activate all the routing nodes. This scheme is used by the initiator to remove an action message. The nonce is asked to prevent a DoS attack by continuity broadcasting action messages.

- Before getting an action message, a node needs to check the last time is less than the message time. It could be done when the signature message is valid.
- If both messages are valid, the node updates the nonce and stores the seed. The node will perform as an collector at the designated time and also operates a claim message for neighboring node (examinee) and passes the message through the overlay network.
- When the nodes starts to forward the claiming message there is chance for large traffic that may causes interference and degrade the network capacity.

Processing Claim's Information: Claim message will be transmitted to its end node via between nodes.

- Those nodes lies in the overlay Intermediate nodes and the end node which can process a message, whereas other nodes in the path simply route the message to temporary targets.

Performance Evaluation:

Throughput: It calculates particular quantity of data transmission over the network, including total quantity of data forward from CH towards a sink and vice versa.

Packet Loss Ratio: It can calculate the total robustness of protocol used in the proposed scheme. It achieved by the dividing percentage of packets loss by the total transmitted packets.

Delay: The network delay calculated by total amount of time taken for a data bit transmission from one node to another node. It is commonly measured fractions of seconds.

Overhead: Overhead is any composite of waste or time, memory, bandwidth, or other resources that are required to attain a particular goal.

3. EXPERIMENTAL RESULT

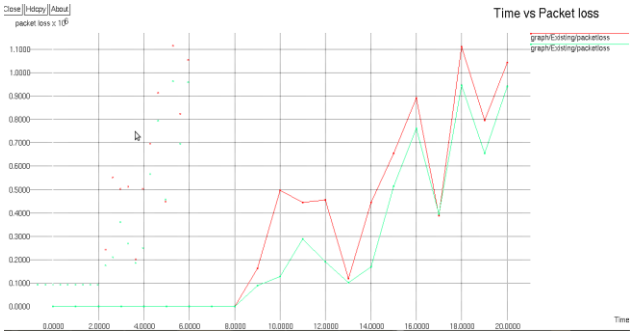

Figure.2. Packet loss

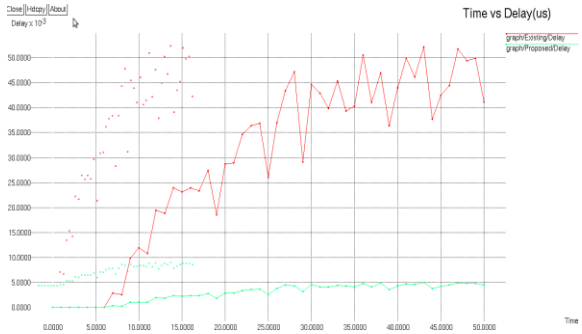

Fig.3. Delay

In fig.2, shows the comparison graph of packet loss with the existing system. Time and packet drop will be plotted along x axis and y axis. The packet drop ratio gets decreased.

In fig.3, describes the comparison graph of the delay with the existing system. Time and delay are plotted in x axis and y axis. The delay gets loss in proposed system

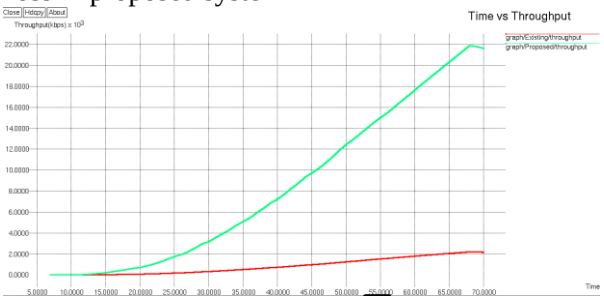

Figure.4. Throughput

In fig.4, shows the comparison graph of throughput with the existing system. Time and throughput will be plotted on x axis and y axis. The throughput gets decreased when compared with the existing system.

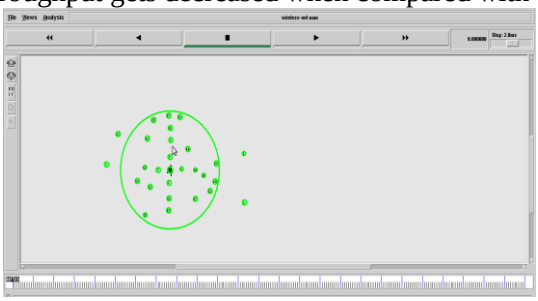

Figure.5. Node formation

In fig.5, designs a route with horizontal direction in a ring path. This establishment test whether the detection route encounter the known path because the distance between witness paths is larger than discover route.

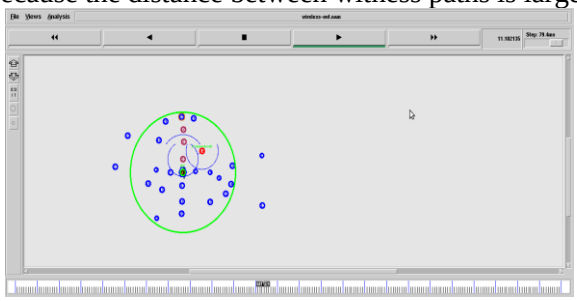

Figure.6. Data transfer with clone node

In fig.6, data can be transfer from one to nearby node. Each node pass its identity to a set of nodes that act as a known node. If the node has a same ID is considered as a captured node but they may be in different location.

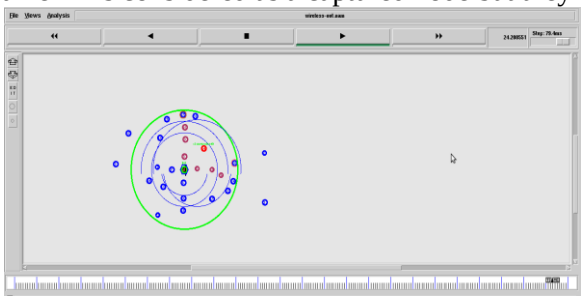

Figure.7. Data transfer without clone node

In fig.7, data can be transfer from one to nearby node. Any node has different ID and location. Therefore there is no clone node.

4. CONCLUSION

Enhanced Random Walk process depends on cloned detection protocol whose storage requirement is only a small constant. Thus protocol successfully achieving a small constant storage requirement. Based on the logical study and experimental results, the Enhanced Random Walk protocol is proven to improve various performance indicators namely, the network lifetime is increased by 20, the Detection probability is increased by 50%, and storage requirements are only 1/5 those of the LSM protocol.

REFERENCES

Liu Y, Liu A and He S, A novel joint logging and migrating trace back scheme for achieving low storage requirement and long lifetime in WSNs, AEU Int. J. Electron. Commun., 69 (10), 2015, 1464–1482.

Luo J, Zhou L and Wen H, Lightweight and effective detection scheme for node clone attack in wireless sensor networks, IET Wireless Sensor Systems, 1 (3), 2011, 137-143.

Sindhukavi K, Brundha P, Beslin pajila P.J, An efficient cloning detection protocol using distributed hash table walk for cyber-physical system in WSN, International journal of scientific research in science engineering and technology, 5 (10), 2016.

Zeng Y, Cao J, Zhang S and Guo S, Random-walk based approach to detect clone attacks in wireless sensor networks, IEEE J. Select. Areas Commun., 28 (5), 2010, 677-691.

Zhu B, Jojodia S, Roy S, Wang L, Localized multicast: efficient and distributed replica detection in large-scale sensor networks, IEEE Transactions Mobile Comput., 9 (7), 2012, 913-926.