ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 3, February 2017

DETECTION OF CLONE BETWEEN CLIENT SERVER IN SECURED SHORTEST PATH

S.Janupriya,
PG Scholar,
Department of Information Technology,
Francis Xavier Engineering College,
Tirunelveli, Tamilnadu, India,
sjanu94@gmail.com

Dr.R.Ravi,
Head of the Department
Department of Information Technology,
Francis Xavier Engineering College,
Tirunelveli, Tamilnadu, India,
cshod@gmail.com

Abstract : Wireless sensor networks (WSN) are spatially distributed autonomous sensors that monitor physical and environmental conditions.An WSN incorporates a gateway that provides wireless connectivity to the distributed nodes. An energy –efficient location-aware clone detection protocol is being proposed thus it support clone detection with efficient network lifetime. The location information of the sensors are being exploited and witnesses are being selected randomly, this verifies the legitimacy. Hence the clone attacks can be reported. For an successful clone detection, selecting the witness and verifying the legitimacy are most required.The sensors are placed in a ring structure so that data forwarding is energy efficient near the path of the sink. In existing protocols, the buffer storage and node density are dependent on each other but considering the proposed the buffer storage is independent. The traffic load is being distributed along the network so that the network lifetime will be efficient.

Keywords: WSN, location aware, network lifetime

I.INTRODUCTION

Wireless sensors are being used in variety of applications in this digital world. But sensors are not properly maintained and this leads to different attacks for sensor nodes. Sometimes the sensor nodes are being duplicated which are meant as clones. The same data from the original sensor is present in the clone. So that the sensors can easily interfere in the network operation and gain their needs. Since the sensor duplication process is so cheap the clone attacks has become a very common issues. Hence detection of clone is essensial for wireless networks.

The initial process for the clone detection is to select a set of nodes known as witnesses. By witnesses selection the legitimacy of the nodes can be certified. The secrecy information can be shared with the witnesses selection process. The data transmission process can be made possible with many steps. The first is to send request for the witnesses so that the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 3, February 2017

legitimacy can be verified. If so it is not verified, the witnesses reports the attacks.For the clone detection process to be completely fulfilled two process have to be carried out. They are (a) random selection of the witnesses; (b) The verification messages have to be send to atleast one of the witnesses. The first process destructs the communication between the witnesses and the node at present. Hence duplicate verification messages can be avoided. The second process is for the authentication purpose. By this the clone detection probability can be established.

For an efficient clone detection process, not only security by network lifetime also plays a vital role. The energy consumption and memory storage is also considered for a proper clone detection process. The clone detection protocol can also be used in multihop wireless sensor networks where there is a occurrence of more attacks. To achieve a high clone detection, a energy-efficient ring based clone detection is being proposed that also ensures network lifetime and selecting witnesses. The process is divided in to two stages; (a) selecting witnesses; (b) verifying legitimacy. In the first stage, the private information are send from the soarce node to the witnesses that are selected randomly by the mapping function.

II. RELATED WORKS

In this section a review of different clone detection techniques and performance parameter are being described.

The survey of clone detection describes that it can be categorised in to two. They are centralised and distributed clone detection protocols. In the centralised clone detection process the sink or the witnesses mainly focusses on the centre of the region for the storage of the private information. For the centralised clone detection protocol, they have low overhead and complexity problems. The privacy could not beguaranteed in centralised clone detection process.The network lifetime may also be decreased due to lot of energy consumption.

In distributed clone detection protocol, it prevents the transmission between the sink and the sensors. The selection of witnesses can be categorised into three types. They are selection by deterministic, selection by random, selection by semi-random.

We can achieve a high clone detection probability with low communication overhead when we make use of deterministic selection. The buffer requirement is also very low that does not considers network scale and node density. The mapping function can be easily obtained by the deterministic property. The deterministic and random in combination increases the network security.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 3, February 2017

In random clone detection protocol, it is difficult to acquire information of witnesses because they are generated randomly. However they also have a drawback that it is difficult for the soarce node to reach the witnesses. The most important is to guarantee clone detection with minimum energy consumption and required buffer storage.

Both of the phases may lead to high overhead and time complexity.The energy consumption and the buffer storage is low in case of random and high for deterministic selection.In this paper both random and deterministic are made use as a distributed system that considers better network lifetime and data buffer capacity.

III . PROPOSED SCHEME

The main aim of the thesis is to reduce the probability of the clone in the networks. This process consists of a central base station (BS) with large number of wireless sensor networks around it. The whole process of system coordination is left to the sink nodes. Based of sink location, the networks are virtually changed into adjacent rings.The network is designed in such a way that (A) the sensor nodes are present in the neighbour nodes of each nodes; (B) There are sufficient sensors to construct a routing path along the ring. The extension can be made through orthogonal frequency-division multiple access (OFDMA) for communication with the sensor nodes. The transmission of data between the sink nodes and the data sensors are possible by the multi-hop paths. Buffer storage should be sufficient for storing the private information. If so the memory is full the old data will be dropped out so that it accepts the new data.

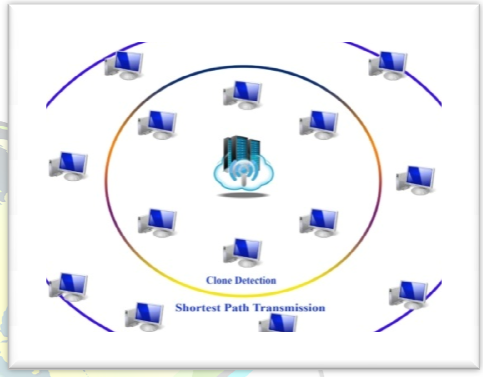

Figure 1 Overview of Clone Detection

Figure 1 portrays the single base station with numerous amount of sensors around it. The first adjacent circle describes about the clone detection process. The second adjacent circle describes about the transmission of data by the shortest path.

3.1 METHODOLOGY

To achieve a high clone detection with good network lifetime and limited buffer storage, a distributed clone detection protocol namely ERCD is being used. The ERCD initiates by the breadth-first search that is the sink node to initiate the ring index. For each an every transmission of data the ERCD protocol is run. In selecting the witnesses the mapping

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 3, February 2017

function is selected from the ring index. The mapping function cannot be selected from the area around the sink node. Next the node sends a private information to the node of witness ring then the information is forwarded as along the witness ring so that it forms a ring structure for easy communication between the nodes. For verification of the legitimate, a verification message from the soarce is forwarded to the witnesses ring. The above process is repeated till the number of rings being present around the base station. The intimation will be made as a message when they are close to the witness ring called as three-ring broadcast. The three-ring broadcast serves for three purpose. The first is the probability of clone detection that whether the witness are trustful. Secondly, to check whether there present a clone attack by ERCD. Finally the recover mechanism by ERCD protocol. If so the clone detection is not possible due to clone attack, the new route is being selected to forward the messages to the witness header.

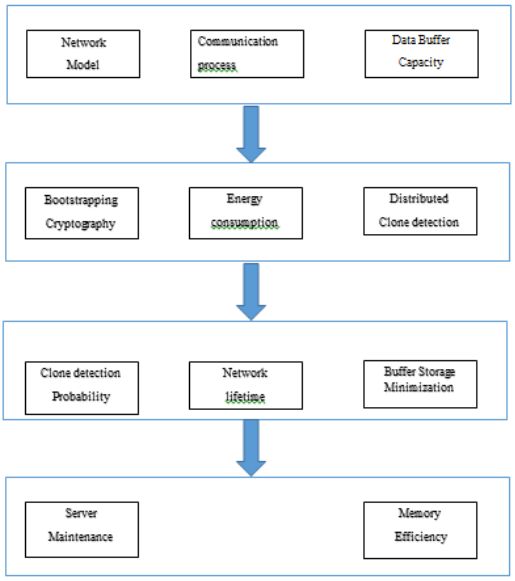

Figure 2 Block Diagram of Witnesses and Legitimacy

The **Figure 2** portrays the steps regarding the model, clone detection, lifetime of network and storage.

i)Clone Detection Probability

The clone detection probability id generally referred to as the witnesses that can successfully receive the messages from the source node. Thus by ERCD protocol it implies the probability that the verification messages are transmitted from the source to the witnesses. The verification messages are being telecasted when they are near the ring of witness such that it guarantee security for the network. By this process we can be satisfied that atleast one of the node will get the verification message. To make it a simple, the transmission of every sensors are same.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 3, February 2017

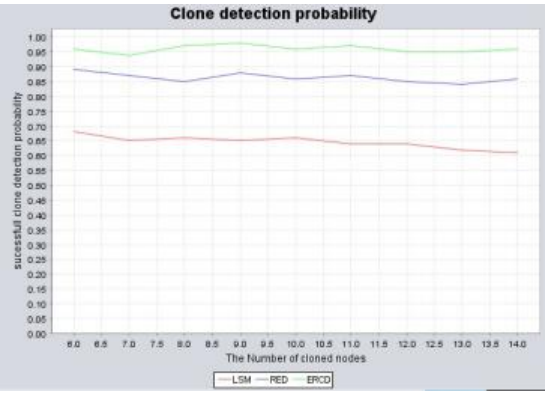

Figure 3 Performmance of Various Clone Detection Protocol

The **Figure 3** gives a comparison of various clone detection protocol being employed in the network. The ERCD gives a better performance than Randomized Efficient and Distributed Protocol(RED) and Line Select Multicast Protocol (LSM)

ii) Energy usage and lifetime of network

The wireless sensor networks are basically being energised with the batteries. So it is hectic to evaluate the energy being consumed and to conform that the network operations are not being broken down by the node outage. Therefore the network lifetime is being defined as the stage from the starting of network operation till the node outage. This network lifetime evaluate the performance of the protocol. The transmission power is alone being considered since the reception power consumption takes only very little energy. The whole setup is being operated in a ring structure, the sensors also performs their task as a ring structure. If there a possibility of traffic load in the same ring, the process is carried out as a different ring structure. The rings are arranged in the order from the smaller to the larger. Initially the traffic load is being analysed so that the energy consumption and network lifetime can be extracted from it.

The network lifetime outperforms other protocols. The packets are being successfully distributed amoung the network except the non-witness area. The protocol is independent of the node degree average. This conforms that the network lifetime doesnotaffect the node density. Like the same way the maximum energy consumption will not affect the average node density.

iii) Capability of Data Buffer

Basically sensors are smaller in size and with low capacity of data and battery backup. The data buffer capacity of the sensors are being evaluated for the performance of the ERCD protocol. Basically the sensor nodes that are near the sink node are heavier in traffic than that they are away from it. This will deplete the energy very fast. But in ERCD the traffic is being distributed along the network hence the energy is being balanced. By this a best network lifetime is achieved.

IV RESULTS AND DISCUSSION

Basically the network consists of many clones that resembles to be the original. Fig 1 indicates the number of nodes that are alive on the network. So that the processing can be easily be discovered.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 3, February 2017

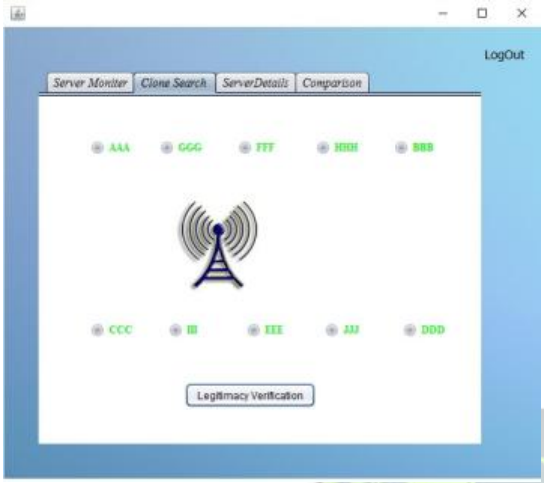

Figure 1 Clone Detection between the Client Server

The above figure shows the nodes which are available to the main server

Figure 2 The details regarding the server is being displayed. The IP address, energy and memory are the different parameters being displayed. Since the legitimacy is being verified, the clone is easily being verified.

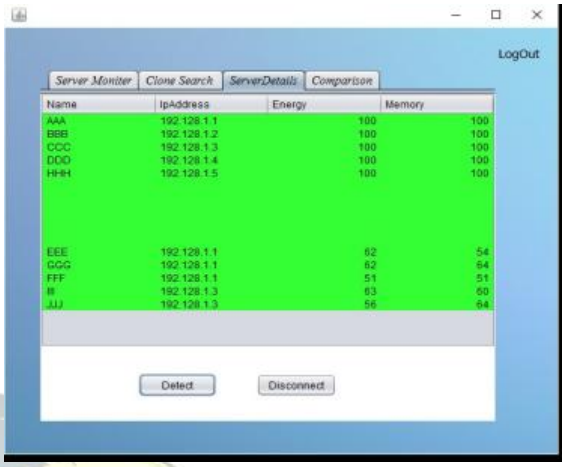

Figure 2 Seperation of Clone from the Original node

The clone is being identified from the list of nodes.

Figure 3 The efficient working of the network totally depends upon the memory and energy that are being used up by the network. The energy used up by each of the network are listed separately.

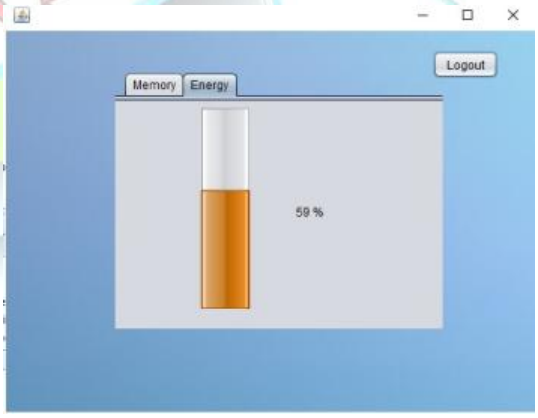

Figure 3 Energy and Memory Usage of Client

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 3, February 2017

The above figure shows the energy and memory level being used up by the nodes.

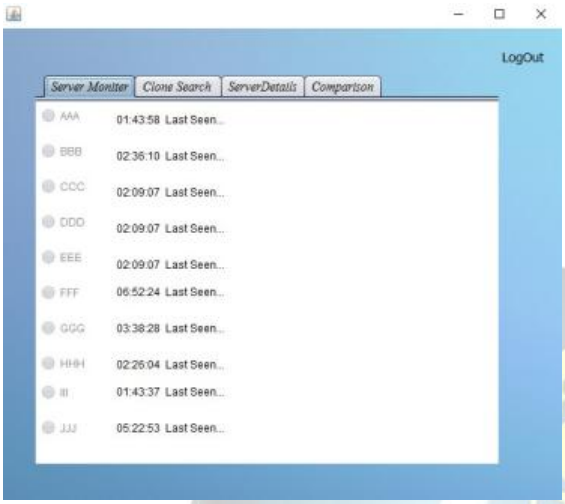

Figure 4 Server Monitoring

The above figure shows the control of the Server towards the Client. Hence the details of all the client is visible through the server login which is kept as private.

Figure 5 Server Login

V. CONCLUSION

This paper introduces the new methodology for the detection of clone between the client and the server. The developed scheme totally relies on the ERCD algorithm. This algorithm helps in saving the energy used up by the nodes and also the efficiency of the nodes. Hence this paper supports green computing which is more important for the current environmental situation. The past survey has concentrated only upon the clone detection process but this algorithm helps for detecting the clone with minimum energy utilization and also for efficiency purpose. The future work is about to send and receive information with out viral in a secured way. We have proposed the ERCD protocol, which includes the witness selection and legitimacy verification stages. In the future work, the data can be send to the client in a shortest path. Hence this process saves time too. The traffic load is also maintained amoung the network since the load is not put upon the single node. The load is being shared amoung all the nodes.

REFERENCES

[1]. 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",Computer Networks, vol. 56, no. 7, pp. 1951-1967, May. 2012.

[2] B.Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 3, February 2017

attacks in sensor networks", in Proc. IEEE Symposium on Security and Privacy, pp. 49-63, May. 2005.

[3] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks", IEEE Transactions on Mobile Computing, vol. 9, no. 5, pp. 913-926, Jul. 2010.

[4] C. Ok, S. Lee, P. Mitra, and S. Kumara, "Distributed routing in wireless sensor networks using energy welfare metric", Information Sciences, vol. 180, no. 1656-1670, May 2010.

[5] H. Chan, A. Perrig, and D.Song, "Random key predistribution schemes for sensor networks" in Proc. Symposium on Security and Privacy, pp. 197-213, May. 2003.

[6] I. F. Akyildiz, W. Su, y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, vol. 38, no. 4, pp. 393-422, Mar. 2002.

[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] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks", in Proc. IEEE ICNP, pp. 284-293, Oct. 2009.

[9] 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. 677-691, Jun. 2010.

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