International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

# Energy and Memory Efficient Clone Detection with Multiple Witness Headers

Penumaka Rama Bhargavi & Dr. S.Jhansi Rani

M.Tech Student Department of Computer Science& Systems Engineering AU College of Engineering (A), Andhra University, Visakhapatnam.
Assistant Professor Department of Computer Science& Systems Engineering AU College of Engineering (A), Andhra University, Visakhapatnam.

**ABSTRACT :**

*Wireless sensor networks [WSNs] have become very popular and ubiquitous technologies for everyday applications. WSNs are vulnerable to clone node attacks that effects in many devastating ways. An attacker can capture a sensor node to install number of clone nodes with same privacy information causing serious security threats and deterioration in network lifetime. Current security scheme along with distinct advantages suffer from number of limitations. A good counter attacks measure should not only cater for security and energy-efficiency but network lifetime as well. Most of the previous works aim at maximizing the clone detection probability without considering the impact of proposed clone detection protocol on the network lifetime and required data buffer storage. Hence we carefully design a distributed clone detection protocol with random witness selection by jointly considering the clone detection probability, network lifetime and data buffer capacity.*

## INTRODUCTION :

Wireless sensor networks (WSNs) have emerged as promising technologies for numerous applications in civil and military. Secure communication is one of the most challenging and risky tasks. WSNs are found to be prone to clone node attacks that effects in many harmful ways. In a clone node attack, an adversary captures a node and installs its code with same privacy information. Later adversary makes multiple copies of the node and installs them throughout the network to take control of the network. If these clone nodes are not detected, network is left vulnerable to attacks and thus severe damage.

In most cases, the sensors forming these networks are deployed arbitrarily and left unattended to and are expected to perform their mission properly and with efficiency. As a results of this random readying, the WSN has typically varied degrees of node density on its space. Sensor networks also are energy strained since the individual sensors that the network is created with, are extraordinarily energy-constrained moreover. The communication devices on these sensors are

little and have restricted power and range.

Wireless sensor network is an insecure to the node replication. We have to detect and report the duplicate node attack in the wsn. The ring structure facilitates energy-efficient data forwarding along the path towards the witnesses and the sink. To prolong network lifetime, i.e., time duration from the start of network until the first occurrence of a sensor that runs out of energy, it is critical to not only minimize the energy consumption of each node but also balance the energy consumption among sensors distributively located in different areas of WSNs.

**ERCD PROTOCOL:**

ERCD protocol can achieve a high clone detection probability with little negative impact on network lifetime and limited requirement of buffer storage capacity. Witness node used in verification of privacy information is randomly selected from a ring area to detect these attacks. Ring structure is used for energy-efficient data forwarding towards the witness node, witness header, and sink or base station (BS). It can also balance the energy consumption of sensors at different locations by distributing the witnesses all over WSNs except non-witness rings, i.e., the adjacent rings around the sink, which should not have witnesses. After that, we obtain the optimal number of non-witness rings based on the function of energy consumption.

Two important phases in existing system are witness selection and legitimacy verification. In witness selection, a random mapping function is employed to help each source node randomly select its witnesses. In the legitimacy verification, a verification request is sent from the source node to its witnesses, which contains the private information of the source node. Here witness headers are nodes responsible for determining whether the source node is legitimacy or not by comparing the messages collected from all witnesses.

**Drawbacks:**

- Sensors use up their batteries quickly due to the unbalanced energy consumption, and dead sensors may cause network partition, which may further affect the normal operation of WSNs.
- Most existing approaches will improve the productive clone detection at the expense of energy consumption and memory storage, which cannot be appropriate for a few sensing element networks with restricted energy resource and memory storage.

**METHODOLOGY:**

The ERCD protocol consists of 2 stages: witness choice and legitimacy verification. In witness choice, a random mapping operates is used to assist every supply node every which way choose its witnesses. within the legitimacy verification, a verification request is distributed from the supply node to its witnesses, that contains the personal info of the supply node. If witnesses receive the verification messages, all the messages are going to be forwarded to the witness header for legitimacy verification, wherever witness headers are nodes liable for deciding whether or not the supply node is legitimacy or not, by comparison, the messages collected from all witnesses. If the received messages are completely different from existing record or the messages are terminated, the witness header can report a clone attack to the sink to trigger a revocation procedure.

**ERCD WITH MULTIPLE HEADERS:**

- Most previous works assume that all selected witnesses are trustful. In our work, we have relaxed the assumption of trustful witness node, and investigated the case that some selected witnesses have been compromised. In ERCD protocol, since we have a set of witnesses for each sensor, the probability that a compromised witness receives the request message is very low.
- An energy and memory-efficient distributed clone detection protocol with random witness selection scheme with multiple witness headers in WSN's.
- In ERCD, the witness header is bottle neck of the scheme, since after a witness header of a witness ring energy level reaches to zero or compromised, it could not work.
- We introduce multiple witness headers to further distribute the energy usage and load balancing. Since, verification can be performed alternatively or another witness header among three is used after one energy level drops to threshold, our proposed scheme will balance the network energy usage in a better way.
- Following are the expected contributions of our proposed method as compared to ERCD.
  1. Network lifetime improvements
  2. Energy efficiency
  3. Traffic load balancing with multiple witness header

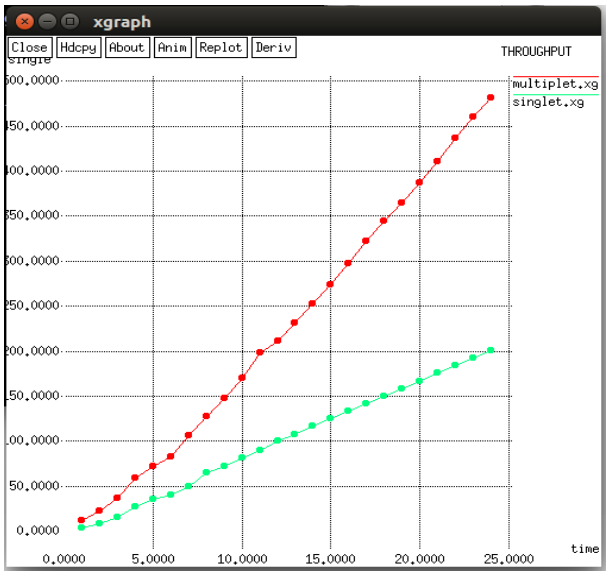
**EXPERIMENTAL RESULTS:**

The performance of ERCD protocol is analysed NS2 open source modular simulation platform in large network. As NS2 is a discrete event-driven system, the event set is stored in the system and events are released one by one to evaluate our ERCD protocol in the simulation.

1. Throughput: At certain intervals of time the

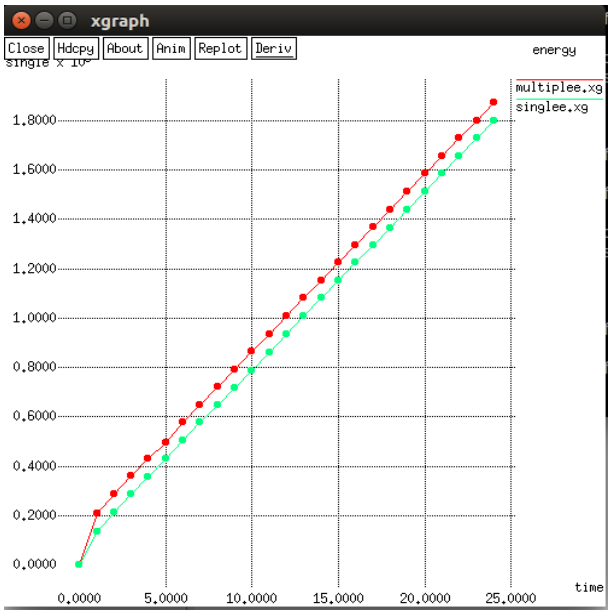
International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

throughput was observed for single witness header and multiple witness headers. The amount of data packets transmitted between the nodes were noted high for ercd with multiple witness headers. The points plotted were drawn a graph as shown below.




2. Energy:

In terms of energy also its proved that ercd protocol with multiple witness headers shows high energy preservance than ercd protocol with single witness headers with same buffer capacity. The points were taken at certain intervals of time and corresponding graph was plotted as shown.




## 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. It can also achieve long network lifetime by effectively distributing the traffic load across the network, energy consumption with the reasonable storage capacity of the data buffer. Both of our theoretical analysis and simulation results have demonstrated that our protocol can detect the clone attack with almost probability with a set of nodes selected within ring area, which are called witness nodes, used to certify the legitimacy of the nodes in the network.

## FUTURE WORK:

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, impact of data aggregation etc.

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

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 Trans. Mobile Comput., vol. 9,no. 7, pp. 913–926, Jul. 2010.

4. 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.

5. B. Parno, A. Perrig, and V. D. Gligor. Distributed detection of node replication attacks in sensor networks. In Proceedings of 2005 IEEE Symposium on Security and Privacy (S&P '05), pages 49–63, 2005.

6. Wazir Zada Khan, Mohammed Y. Aalsalem, Mohammed Naufal Bin Mohammed Saad, and Yang Xiang,—Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey, pp. 1-22, vol.2013, 2013.

7. Zhijun Li, Member and Guang Gong, —On the Node Clone Detection in Wireless Sensor Networks, IEEE/ACM TRANSACTIONS ON NETWORKING, pp.1799-1811, vol. 21, no. 6, December 2013.

8. 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.

9. R. Lu,X. Lin, X.Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs,"IEEETrans.Intell.Transp.Syst., vol.13,no.1,pp.127–139,Jan.2012.

10. 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