ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 5, Issue 5, May 2018

Enhancing the Network Lifetime and Storage Utilization Using Distributed Clone Detection in Wireless Networks

[1] Choudary Swetha, [2] M Pragathi

[1] M. Tech Student, [2] Associate Professor, [1][2] Department of CSE, Sridevi Women's Engineering College, Village VattiNagulaPally, Mandal Rajendra Nagar, District RangaReddy, Telangana, India

Abstract: **- In this paper, we support an energy-efficient location-conscious clone detection protocol in compactly deployed WSNs that may assurance successful clone assault detection and maintain exceptional network lifetime. In particular, we make the most the province facts of sensors and randomly pick witnesses placed in a ring region to confirm the legitimacy of sensors and to certificate detected clone attacks. The ring structure helps electricity-efficient records forwarding along the path in the direction of the witnesses and the sink. We tentatively prove that the anticipated protocol can obtain one hundred percent clone detection probability with trustful witnesses. In addition, we develop the work by way of reading the clone detection explain with untruthful witnesses and show that the clone detection prospect still strategies 98 percentage when 10 percentages of witnesses are compromised. furthermore, in maximum current clone detection protocols with random witness selection proposal, the required buffer garage of sensors is usually dependent on the node density, i.e., 0 √n, at the same time as in our projected protocol, the specified buffer garage of sensors is impartial of n but a characteristic of The hop period of the network radius h, i.e., 0(h). Widespread simulations display that our planned protocol can accomplish long network lifetime by using efficiently distribute the site visitor's load crosswise the network.**

Key words: - Wireless sensor networks, clone detection protocol, energy efficiency, network lifetime.

I. INTRODUCTION

Presently, Wireless sensors are extensively used in distinctive applications. Wireless networks starting from surroundings monitoring to telemedicine and then network items are tracked. The sensor networks are having the drawback of cost-effective. Because of, sensors do not tamper proof typically. That is the concept hackers can attack the sensors easily. For example, a spiteful person may additionally compromise a few sensors and accumulate their non-public facts. Then, it is able to reproduction the sensors and deploy clones in a wireless sensor network (WSN) to launch a diffusion of assaults. As the duplicated sensors have the identical statistics, e.g., code and cryptographic records, captured from valid sensors, they are able to without problems participate in network operations and launch assaults. Due to the low price of sensor duplication and deployment, clone attacks have emerge as one of the maximum essential safety troubles in WSNs. Thus, its miles vital to effectively come across clone attacks so one can ensure wholesome operation of WSNs. So, we are able to rectify the clone detection with the aid of the usage of vigour memory with proficient wireless networks. We can acquire the set of nodes and decided on based on the witness. The private data of the supply node, i.e., identity and the location records are shared with witnesses on the degree of witness selection. When any of the nodes inside the network desires to transmit data, it first sends the request to the witnesses for legitimacy verification, and witnesses will report a detected attack if the node fails the certification. To gain successful clone detection, witness selection and legitimacy verification must to satisfy two necessities: 1) witnesses should be randomly decided on, and 2) at least one of the witnesses can successfully receive all of the verification messages for clone detection. The first requirement is to make it difficult for malicious customers eavesdrop the conversation between the modern-day source node and its witnesses so that malicious users can not generate duplicate verification messages. The 2d requirement is to ensure that at least one of the witnesses can test the identification of the sensor nodes to determine whether there's a clone attack or now not. The chance that clones attacks can be successfully detected. Different from wireless terminal gadgets, wireless sensors are common for smaller length and decrease fee, and feature constrained battery and memory capability. Therefore, the design principle of clone detection protocols for sensor networks must not valuable assure the high presentation of clone detection risk but additionally don't forget the strength and memory piece of sensors. In the project, a few dispensed clone detection protocols had been proposed, including Randomized Efficient and Distributed protocol (RED) and Line Select Multicast protocol (LSM). However, most approach largely focused on recovering clone detection prospect without consider efficiency and balance of energy expenditure in WSNs. Another form of assault i.e., a few sensors can be their batteries due to unbalanced power intake and lifeless sensors can also purpose network partitions which may additionally similarly have an effect on the everyday operation of WSNs. To lengthen network lifetime, i.e., the time duration from the begin of the network till the first incidence of a sensor that runs out of strength, it is vital to now not simplest limit the power consumption of each node however additionally balance the electricity consumption amongst sensors distributive located in one of a kind regions of WSNs. The restrained reminiscence or information buffer is every other critical feature of sensors which has a substantial effect on the layout of clone detection protocols. Generally, to guarantee hit clone detection, witnesses want to file source nodes personal records and certify the legitimacy of sensors primarily based on the saved private data. In most current clone detection protocols, the specified buffer garage size relies upon at the network node density, i.e., sensors need a huge buffer to file the exchanged records among sensors in a high-density WSN, and consequently, the desired buffer length scales with the network node density. We proposed power intake and reminiscence storage inside the design of clone detection protocol, i.e., an energy and memory-efficient disbursed clone detection protocol with random witness selection scheme in WSNs. Our protocol is applicable to widespread densely deployed multi-hop WSNs, in which adversaries may additionally compromise and clone sensor nodes to release assaults. We proposed an energy-efficient ring based totally clone detection (ERCD) protocol to gain excessive clone detection opportunity with random witness selection while making sure regular network operations with quality network lifetime of WSNs. The ERCD protocol can be divided into two ranges: witness choice and legitimacy verification. In witness selection, the supply node sends its non-public information to a set of witnesses, which might be randomly decided on with the aid of the mapping function. In the legitimacy verification, verification message alongside the personal statistics of the supply node is transmitted to its witnesses. If any of witnesses effectively gets the message, it's going to ahead the message to its witness header for verification upon receiving the messages. The witness header compares the aggregated verification messages with stored statistics. If more than one copy of verification messages is obtained, the clone assault is detected and a revocation procedure can be triggered.

II. RELATED WORK

V.Sathya et al proposed electricity efficient clone detection the use of Iterative Filtering Algorithm and to boom the network lifetime the usage of Sleep- Awake Technique. Compressive Sensing can stability the network traffic. To offer the clustered environment for records aggregation within the wireless sensor network and make strength efficient sensor nodes with strength monitoring. Rongxing Lu et al studied the issues to achieve green M2M communications by employing efficient activity scheduling techniques for energy saving. They had also offered several approaches to address the reliability and security issues in M2M communications. Although they discuss the GRS issues in the broad-spectrum M2M communications paradigm to lean-to light on this research line, further efforts are required to recognize the GRS issues in definite M2M communications contexts e.g., a time-critical and privacy-sensitive e-healthcare system.

Anfeng Liu et al studied cost function based energy-aware routing. They proposed the general principles of cost function design and evaluation criteria. Further, they presented novel energy aware and cost based routing algorithms named exponential and sine cost function based routing (ESCFR) and double cost function based routing (DCFR). These two algorithms aim at maximizing the lifetime of the network by means of power consumption equalization. Comprehensive simulation results demonstrate that the algorithm can significantly improve network lifetime comparing with the best solution known in the literature, such as DC, MTE, and DEBR.

A novel prompt classification service for reactive jamming attack in wireless sensor network is introduce to achieve minimum time and message transparency. The status report message is transferred between the base station and all sensor nodes. For isolating reactive jammer in the network a trigger identification service is introduced, which requires all testing groups to schedule the trigger node detection algorithm using group testing after anomaly detection. By identifying the trigger nodes in the network; automatic jammers can be eliminated by assembly trigger nodes as only receivers. This detection scheme is thus well-suited for the protection of the sensor network against the reactive jammer. Furthermore, an investigation into more stealthy and energy efficient jamming models with simulations indicates the robustness of the present proposed scheme. The result can be stored in the network for further operations i.e. to perform best routing operation without jamming. This work achieves the elimination of attackers to maintain the soundness of wireless sensor networks.

III. FRAMEWORK

A. ERCD protocol

The ERCD protocol is likewise called a disbursed protocol that could enhance the excessive clone detection opportunity with little bad impact on network life and confined requirement of buffer garage capacity. The ERCD protocol includes degrees: witness selection and legitimacy verification. In witness choice, a random mapping feature is hired to assist each source node randomly choose its witnesses.

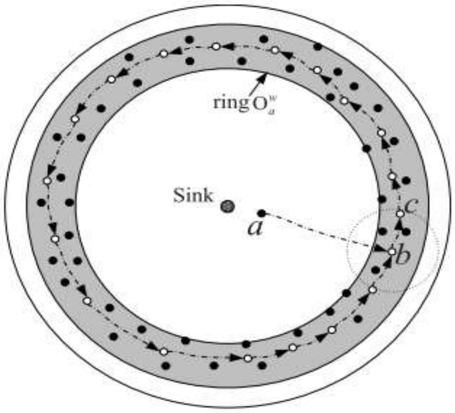


Fig: 1 Ring Structure of witness

In the legitimacy verification, a verification request is sent from the source node to its witnesses, which includes the personal data of the supply node.

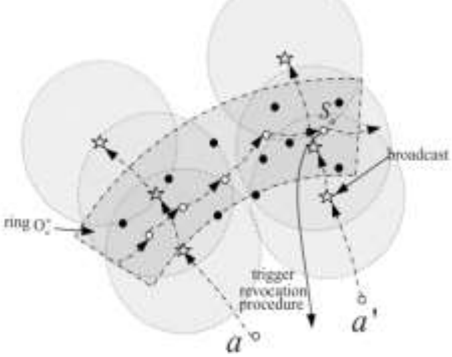


Fig.2 Legitimacy verification

If witnesses receive the verification messages, all of the messages will be forwarded to the witness header for legitimacy verification, wherein witness headers are nodes answerable for figuring out whether or not the supply node is legitimacy or no longer through evaluating the messages accrued from all witnesses. If the received messages are different from current file or the messages are expired, the witness header will document a clone attack to the sink to trigger a revocation process.

B. Probability of Clone Detection

The clone detection chance usually refers to whether or not witnesses can efficaciously receive the verification message from the source node or not. Thus, the clone recognition prospect of ERCD protocol is the chance that the substantiation message can be productively transmitted from the supply node to its witnesses. In ERCD protocol, the verification message is broadcast when it is near the witness ring.

C. Energy Consumption and Network Lifetime

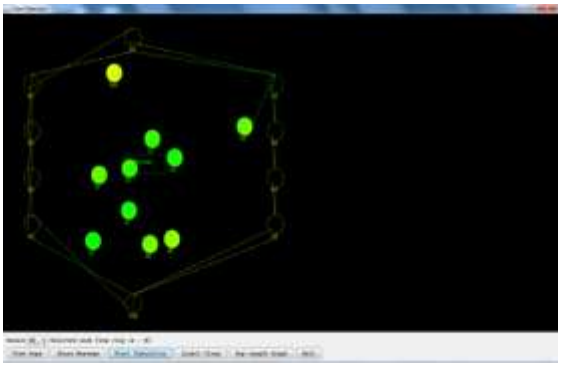
In WSNs, since wireless sensor nodes are generally powered with the aid of batteries, it's far vital to assess the energy intake of sensor nodes and to ensure that normal network operations will not be broken down by means of node outage. Therefore, we define the network life as the duration from the start of network operation till any node outage takes place to evaluate the overall performance of the ERCD protocol. We simplest do not forget the transmission power consumption because the reception power consumption occupies a touch percentage of total electricity intake. Since witness units in our ERCD protocol are generated primarily based on ring shape, sensor nodes in the equal ring have similar tasks.

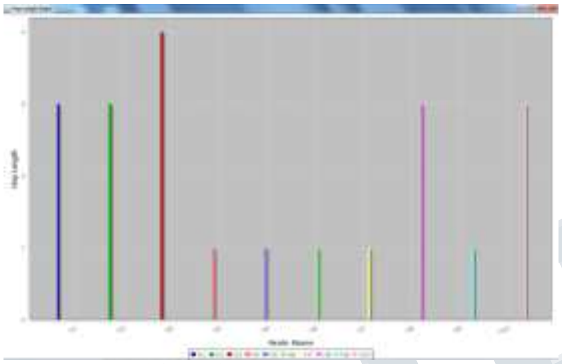
D. Data Buffer Capacity

Usually, sensors are of small size and have a completely confined ability of both facts buffer and electricity battery. In this section, we analyze the desired records buffer capacity, additionally known as statistics buffer of sensors to assess the overall performance of the proposed ERCD protocol. Let s denote the desired packet storage size for being a witness of a sensor node.

IV. EXPERIMENT RESULTS

In this experiment, we have to create wireless sensor network. To create network, we need to enter the network size then network created with given range of nodes. The view hops show the closest nodes for every node and calculate the gap from each node to sink node. Select some sender node then begin the simulations. Then one node verification fulfilment every other failed as it is clone node. Then graph will suggest that how many witnesses can be to be had for every node.





V.CONCLUSION

We have proposed ERCD protocol, which includes the witness selection and legitimacy verification ranges. Both of our theoretical evaluation and simulation effects have proven that our protocol can discover the clone attack with nearly possibility 1 since the witnesses of each sensor node are distributed in a hoop structure which makes it clean be done by using verification message. Our protocol can acquire better network lifetime and overall electricity consumption with a reasonable garage potential of the facts buffer. By distributing the traffic load throughout WSNs, such that the power consumption and memory garage of the sensor nodes around the sink node may be relieved and the network life can be prolonged.

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. R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," IEEE Commun. Mag., vol. 49, no. 4, pp. 28–35, Apr. 2011.

3. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Comput. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002.

4. 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.

5. T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

6. P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 7, pp. 1036–1045, Sep. 2010.
7. R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012.

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," IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127–139, Jan. 2012.

10. 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