WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secured and Enhance Data Sharing in Wireless Sensor Networks Using Clone Model

Dr. Masrath Begum[1], Revathi[2], Shweta[3], Swati[4], Vaishnavi Kathare[5]

Assistant Professor[1], Reader GNDEC Bidar, India.
Associate Professor, VTUCPGS, Karnataka, India. masrathcse@gmail.com,

ABSTRACT:

As sensor nodes deployed for a variety of applications, cost effective and malicious user may compromise some sensors and acquire their private information. As the duplicated sensors have the same information they can easily participate in network operations and compromise of attacks. So we have proposed distributed energy-efficient clone detection protocol with random witness selection. ERCD protocol, which includes the witness selection and legitimacy verification stages. The nodes in the network wants 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. This work is used to send the data from source to destination by creating the clone of that particular data. The strategy ought to find the clone in this way to keep up a key separation from the duplicate center pointer to recognize the packages. To provide the security to client data. The main objective of the project is to protect the data from unwanted malicious error. In present system among many physical attacks to sensor networks, the node clone is a serious and dangerous one. Insufficient storage consumption performance in the existing system and low security level.

Whereas in proposed work the DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks. Randomly directed exploration, is intended to provide highly efficient communication performance with adequate detection probability for dense sensor networks.

Keywords **—ERCD, DHT, wireless sensors, cloud computing**

I. INTRODUCTION

An energy-efficient location-aware clone detection protocol in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically, we exploit the location information of sensors and randomly select witnesses located in a ring area to verify the legitimacy of sensors and to report detected clone attacks. The ring structure facilitates energy-efficient data forwarding along the path towards the witnesses and the sink. We theoretically prove that the proposed protocol can achieve 100 percent clone detection probability with trustful witnesses. We further extend the work by studying the clone detection performance with untrustful witnesses and show that the clone detection probability still approaches 98 percent when 10 percent of witnesses are compromised. Moreover, in most existing clone detection protocols with random witness selection scheme, the required buffer storage of sensors is usually dependent on the node density, while in our proposed protocol, the required buffer storage of sensors is independent of number of nodes but a function of the hop length of the network radius h. Extensive simulations demonstrate that our proposed protocol can achieve long network lifetime by effectively distributing the traffic load across the network.

II. BACKGROUND STUDY

WIRELESS sensors have been widely deployed for a variety of applications, ranging from environment monitoring to telemedicine and objects tracking, For cost-effective sensor placement, sensors are usually not tamper-proof devices and

are deployed in places without monitoring and protection, which makes them prone to different attacks. For example, a malicious user may compromise some sensors and acquire their private information. Then, it can duplicate the sensors and deploy clones in a wireless sensor network (WSN) to launch a variety of attacks, which is referred to as the clone attack. As the duplicated sensors have the same information, e.g., code and cryptographic information, captured from legitimate sensors, they can easily participate in network operations and launch attacks. Due to the low cost for sensor duplication and deployment, clone attacks have become one of the most critical security issues in WSNs. Thus, it is essential to effectively detect clone attacks in order to ensure healthy operation of WSNs.

III. RELATED WORK

Z. Zheng, A. Liu, L. X. Cai, Z. Chen, X. Shen, "ERCD: An energy-efficient clone detection protocol in WSNs", *Proc. IEEE INFOCOM*, pp. 2436-2444, Apr. 2018.

Wireless sensor networks (WSNs) play an increasing role in a wide variety of applications ranging from hostile environment monitoring to telemedicine services. The hardware and cost constraints of sensor nodes, however, make sensors prone to clone attacks and pose great challenges in the design and deployment of an energy-efficient WSN. In this paper, we propose a location-aware clone detection protocol, which guarantees successful clone attack detection and has little negative impact on the network lifetime. Specifically, we utilize the location information of sensors and randomly select witness nodes located in a ring area to verify the privacy of sensors and to detect clone attacks. The ring structure facilitates energy efficient data forwarding along the path towards the witnesses and the sink, and the traffic load is distributed across the network, which improves the network lifetime significantly. Theoretical analysis and simulation results demonstrate that the proposed protocol can approach 100% clone detection probability with trustful witnesses. We further extend the work by studying the clone detection performance with untrustful witnesses and show that the clone detection probability still approaches 98% when 10% of witnesses are compromised. Moreover, our proposed protocol can significantly improve the network lifetime, compared with the existing approach.

R. Lu, X. Li, X. Liang, X. Shen, 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. 2017.

Machine-to-machine communications is characterized by involving a large number of intelligent machines sharing information and making collaborative decisions without direct human intervention. Due to its potential to support a large number of ubiquitous characteristics and achieving better cost efficiency, M2M communications has quickly become a market-changing force for a wide variety of real-time monitoring applications, such as remote e-healthcare, smart homes, environmental monitoring, and industrial automation. However, the flourishing of M2M communications still hinges on fully understanding and managing the existing challenges: energy efficiency (green), reliability, and security (GRS). Without guaranteed GRS, M2M communications cannot be widely accepted as a promising communication paradigm. In this article, we explore the emerging M2M communications in terms of the potential GRS issues, and aim to promote an energy-efficient, reliable, and secure M2M communications environment. Specifically, we first formalize M2M communications architecture to incorporate three domains - the M2M, network, and application domains - and accordingly define GRS requirements in a systematic manner. We then introduce a number of GRS enabling techniques by exploring activity scheduling, redundancy utilization, and cooperative security mechanisms. These techniques hold promise in propelling the development and deployment of M2M communications applications.

T. Shu, M. Krunz, 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. 2014.

Compromised node and denial of service are two key attacks in wireless sensor networks (WSNs). In this paper, we study data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. We argue that classic multipath routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once the adversary acquires the routing algorithm, it can compute the same routes known to the source, hence, making all information sent over these routes vulnerable to its attacks. In this paper, we develop mechanisms that generate randomized multipath routes. Under our designs, the routes taken by the ¿ shares¿ of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes. We analytically investigate the security and energy performance of the proposed schemes. We also formulate an optimization problem to minimize the end-to-end energy consumption under given security constraints. Extensive simulations are conducted to verify the validity of our mechanisms.

R. Lu, X. Lin, T. H. Luan, X. Liang, 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.

As a prime target of the quality of privacy in vehicular ad hoc networks (VANETs), location privacy is imperative for VANETs to fully flourish. Although frequent pseudonym changing provides a promising solution for location privacy in VANETs, if the pseudonyms are changed in an improper time or location, such a solution may become invalid. To cope with the issue, in this paper, we present an effective pseudonym changing at social spots (PCS) strategy to achieve the provable location privacy. In particular, we first introduce the social spots where several vehicles may gather, e.g., a road intersection when the traffic light turns red or a free parking lot near a shopping mall. By taking the anonymity set size as the location privacy metric, we then develop two anonymity set analytic models to quantitatively investigate the location privacy that is achieved by the PCS strategy. In addition, we use game-theoretic techniques to prove the feasibility of the PCS strategy in practice. Extensive performance evaluations are conducted to demonstrate that better location privacy can be achieved when a vehicle changes its pseudonyms at some highly social spots and that the proposed PCS strategy can assist vehicles to intelligently change their pseudonyms at the right moment and place.

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

Smart grid presents the largest growth potential in the machine-to-machine market today. Spurred by the recent advances in M2M technologies, the smart meters/sensors used in smart grid are expected not to require human intervention in characterizing power requirements and energy distribution. These

numerous sensors are able to report back information such as power consumption and other monitoring signals. However, SG, as it comprises an energy control and distribution system, requires fast response to malicious events such as distributed denial of service attacks against smart meters. In this article, we model the malicious and/or abnormal events, which may compromise the security and privacy of smart grid users, as a Gaussian process. Based on this model, a novel early warning system is proposed for anticipating malicious events in the SG network. With the warning system, the SG control center can forecast such malicious events, thereby enabling SG to react beforehand and mitigate the possible impact of malicious activity. We verify the effectiveness of the proposed early warning system through computer-based simulations.

IV. METHODOLOGY

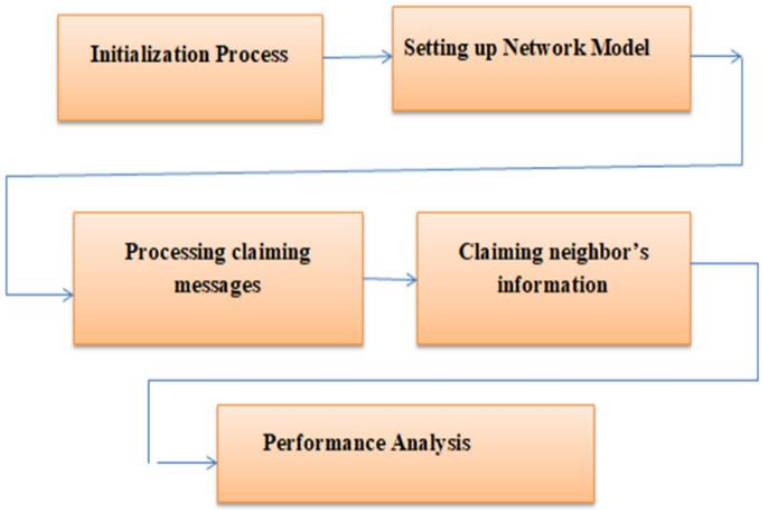

Fig 1: Steps of Methodology

- **Initialization:** To activate all nodes starting a new round of node clone detection, the initiator uses a broadcast authentication scheme to release an action message including a monotonously increasing nonce.
- **Setting up a network module:** Our first module is setting up the network model. We consider a large-scale, homogeneous sensor network consisting of resource-constrained sensor nodes. Analogous to previous distributed detection approaches.
- **Processing claiming messages:** A claiming message will be forwarded to its destination node via several Chord intermediate nodes. Only those nodes in the overlay network layer need to process a message, whereas other nodes along the path simply route the message to temporary targets.
- **Claiming neighbor's information:** At the designated action time, the node operates as an observer that generates a claiming message for each neighbor (examinee) and transmits the message through the overlay network with respect to the claiming probability.
- **Performance analysis:** For the DHT-based detection protocol, the following specific measurements to evaluate its performance:
    - Average number of transmitted messages, representing the protocol's communication cost;
    - Average size of node cache tables, standing for the protocol's storage consumption;
    - Average number of witnesses, serving as the protocol's security level because the detection protocol is deterministic and symmetric.

Module Description:

Legitimacy verification:

In the legitimacy verification, node a sends a verification message including its private information following the same path towards the witness ring as in witness selection. To enhance the probability that witnesses can successfully receive the verification message for clone detection, the message will be broadcast when it is very close to the witness ring, namely three-ring broadcasts.

Clone Detection:

In distributed clone detection protocol with random witness selection, the clone detection probability generally refers to whether witnesses can successfully receive the verification message from the source node or not. Thus, the clone detection probability of ERCD protocol is the probability that the verification message can be successfully transmitted from the source node to its witnesses.

V. DESIGN

System Design is the next development stage where the overall architecture of the desired system is decided. The system is organized as a set of sub systems interacting with each other. While designing the system as a set of interacting subsystems, the analyst takes care of specifications as observed in system analysis as well as what is required out of the new system by the end user.

As the basic philosophy of Object-Oriented method of system analysis is to perceive the system as a set of interacting objects, a bigger system may also be seen as a set of interacting smaller subsystems that in turn are composed of a set of interacting objects.

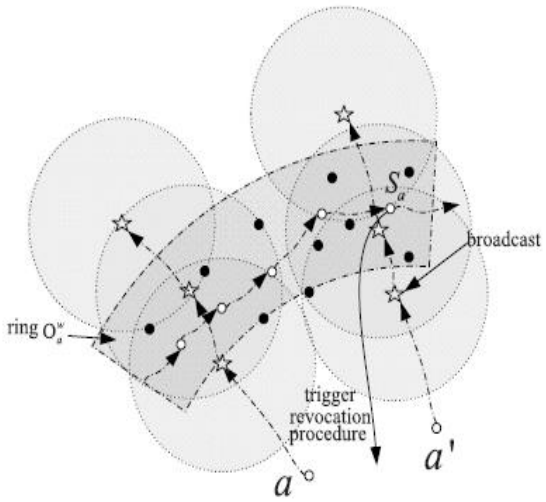

Fig 2: Shows the legitimacy verification

Let an and a' mean the source hub and one cloned hub. The confirmation memos of all and an' are communicate in rings. To enhance the probability that witnesses can successfully receive the verification message for clone detection, the message will be broadcast when it is very close to the witness ring, namely three-ring broadcasts.

VI. CONCLUSION

- NS2 simulator is used for simulation between different nodes securely and efficiently using graphical user interphase (GUI).
- The clone has two sub options such as RUN CLONE and RUN NAM.
- It finds out the shortest path between the two nodes by using NS2 which is better than existing one.
- As compared to all existing systems by using clone model both security and efficiency can be enhanced.

VII. 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] I. 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] 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.

[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. 201