International Journal of Research Publication and Reviews

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

ENERGY EFFICIENT RESOURCEFUL REPLICA DETECTION IN WSN

Prof.Gouri Patil, Amreen Naazneen, Ayesha Begum, Ganesh, Hafsa Fatima

B.E 4th Year, Guru Nanak Dev Engineering College
Email ID: lilcorne786@gmail.com

ABSTRACT

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.

1. INTRODUCTION

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 tamperproof 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.

2. STATEMENT OF PROBLEM

Networking application uses the sensors for the data communication purpose, one of the main component used in the networking communication is sensor, but one of the main limitation of the sensors are the battery usage, as it is remotely operated devices one cannot provide the direct power to it, it has to be operated using the battery. Hence power usage is a main problem as unnecessary power utilization must not happen, many times as sensors usage some kind of ID for identification purpose, these ID's can be used by some unauthorized nodes which will act like clone and steal confidential data from the other nodes, which will cause security breach as well as power wastage.

3. OBJECTIVE OF THE PROJECT

- It should find that, the ER-CD tradition ought to change the imperativeness usage of sensors from dissimilar zones by dispersing the observers with or without over WS-Ns from non-witness rings.
- It should get the perfect number of non-witness rings in perspective of the limit of essentialness use.
- The strategy ought to find the clone in this way keep up a key separation from the duplicate center point to recognize the packages.
- The yield of the system must be awesome appeared differently in relation to the present one.

4. SCOPE OF THE PROJECT

Systems administration application utilizes the sensors for the information correspondence reason, one of the fundamental segment utilized as a part of the systems administration correspondence is sensor, however one of the principle restriction of the sensors are the battery use, as it is remotely worked gadgets one can't give the immediate energy to it, it must be worked utilizing the battery. Subsequently control use is a primary issue as superfluous power use must not occur, ordinarily as sensors use some sort of ID for distinguishing proof reason, these ID's can be utilized by some unapproved hubs which will act like clone and take private information from alternate hubs, which will cause security break and additionally control wastage.

5. 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 endto-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 gametheoretic 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.

6. SYSTEM ANALYSIS

EXISTING SYSTEM

- To allow powerful clone disclosure, generally, a game plan of center points are picked, that are called observers, to assist ensure the validness of the center points in the framework. The confidential data of the source center point, i.e., character and the range data, is granted to observers at the period of witness assurance. Exactly once any of the center points in the framework needs to communicate data. The power utilization is wasted because other nodes use the ID of the other nodes to steal the information from the sensor nodes. This makes the power to be wasted unnecessary.

  The memory is also used a lot because the nodes are unnecessarily stores all kinds of information about the packet which is being transmitted to the destination.

Randomized Efficient and Distributed tradition (RE-D) and LineSelect Multicast tradition (LS-M) experience their batteries in view of the unequal essentialness usage, and dead sensors may cause orchestrate divide, may moreover impact the run of the mill operation of WSNs.

DISADVANTAGES OF EXISTING SYSTEM:

1. It utilizes lots of power as all other nodes just work for the data transmission purpose. All the nodes will be in active mode all time.
2. It does not consider the shortest path for the packet transmission hence it takes lots of time as well as lots of communication power.
3. While transmitting the packets it does not check all the nodes for the node identity hence it may send the packets to the unauthorized nodes also.

PROPOSED SYSTEM:

- Here we consider other than the clone distinguishing proof likelihood, we in like manner consider essentialness usage with memory stockpiling in the diagram of clone revelation tradition, i.e., an imperativeness and memory's profitable scattered clone area tradition with discretionary observer decision arrange in WS-Ns.
- The tradition is suitable to general thickly passed on multi-bounce WS-Ns, these foes will exchange off and clone sensors centers to dispatch strikes.
- The logical model connects by surveying the required data support of ERCD tradition and by counting exploratory results to reinforce our theoretic examination.
- We find that the ER-CD tradition can alter the imperativeness use of sensors, i.e the ID's of each of the node checked before actuelly sending the packets from one node to another node.
- Then the reach of nodes cooperates with each to send the packets with shortest path, so that the power consumption is very less as compared with other protocol.

ADVANTAGES OF PROPOSED SYSTEM:

- The execution of the ER-CD tradition is surveyed similarly as clone area probability, control usage, orchestrate lifetime, and data pad restrain.

- Extensive reenactment comes to fruition display that our proposed ER-CD tradition can finish unrivaled execution in regards to the clone revelation probability and framework lifetime with sensible data support restrain.
- The investigate comes to fruition display so that clone distinguishing proof likelihood can almost method 100 percentage.
- By using ER-CD tradition, essentialness use of sensors near to the destination has cut down action of witness assurance and validness affirmation, which changes the uneven imperativeness usage of data gathering.

7. CONCLUSION

I have considered flowed essentialness gainful clone acknowledgment tradition with subjective witness decision. Exactly, I have considered ER-CD tradition, which consolidates the witness decision and legitimacy affirmation stages. Both of our speculative examination and generation comes to fruition have shown that our tradition can distinguish the clone bout with about likelihood, from the spectators of each sensor center is appropriated in a ring structure which makes it basic be expert by affirmation message. Besides, our tradition can finish better framework lifetime and total essentialness use with sensible limit point of confinement of data pad. That is by virtue of we abuse the range information by spreading the development stack all over WSNs, with the true objective that the essentialness usage and memory stockpiling of the sensors.

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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.