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 17, March 2017

ENERGY AND MEMORY EFFICIENT REPLICA DETECTION IN WIRELESS SENSOR NETWORK

S.THALFIYA NASRIN[1] Dr.C.SUMITHRADEVI [2]

1. PG Student, Dept.of Computer Applications, VSB Engineering College, Karur.
2. Assistant Professor, Dept.of Computer Applications, VSB Engineering College, Karur.

Abstract

An energy-efficient location-aware clone detection protocol is proposed in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically, the location information of sensors is used 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. Proposed protocol can achieve 100% clone detection probability with trustful witnesses. 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 proposed protocol, the required buffer storage of sensors is independent of hop length of the network radius. 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, etc.. 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

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 17, March 2017

to effectively detect clone attacks in order to ensure healthy operation of WSNs.

Different from wireless terminal devices, wireless sensors are usually of smaller size and lower price, and have limited battery and memory capacity. Therefore, the design criteria of clone detection protocols for sensor networks should not only guarantee the high performance of clone detection probability but also consider the energy and memory efficiency of sensors.

To prolong the network lifetime, i.e., the 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 distributive located in different areas of WSNs.

2. LITERATURE SURVEY

Distributed detection of node replication attacks in sensor networks, B. Parno, A. Perrig, and V. Gligor

The low-cost, off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. Such attacks may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighborhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, we propose two new algorithms based on emergent properties (Gligor (2004)), i.e., properties that arise only through the collective action of multiple nodes. Randomized multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, while line-selected multicast uses the topology of the network to detect replication. Both algorithms provide globally-aware, distributed node-replica detection, and line-selected multicast displays particularly strong performance characteristics. We show that emergent algorithms represent a promising new approach to sensor network security; moreover, our results naturally extend to other classes of networks in which

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 17, March 2017

nodes can be captured, replicated and re-inserted by an adversary.

Looking up data in P2P systems: H. Balakrishnan, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica,The main challenge in P2P computing is to design and implement a robust and scalable distributed system composed of inexpensive, individually unreliable computers in unrelated administrative domains. The participants in a typical P2P system might include computers at homes, schools, and businesses, and can grow to several million concurrent participants.

Location-based compromise tolerant security mechanisms for wireless sensor networks: Y. Zhang,W. Liu,W. Lou, andY. Fang, Node compromise is a serious threat to wireless sensor networks deployed in unattended and hostile environments. To mitigate the impact of compromised nodes, we propose a suite of location-based compromise-tolerant security mechanisms. Based on a new cryptographic concept called pairing, we propose the notion of location-based keys (LBKs) by binding private keys of individual nodes to both their IDs and geographic locations. We then develop an LBK-based neighborhood authentication scheme to localize the impact of compromised nodes to their vicinity. We also present efficient approaches to establish a shared key between any two network nodes. In contrast to previous key establishment solutions, our approaches feature nearly perfect resilience to node compromise, low communication and computation overhead, low memory requirements, and high network scalability. Moreover, we demonstrate the efficacy of LBKs in counteracting several notorious attacks against sensor networks such as the Sybil attack, the identity replication attack, and wormhole and sinkhole attacks. Finally, we propose a location-based threshold-endorsement scheme, called LTE, to thwart the infamous bogus data injection attack, in which adversaries inject lots of bogus data into the network. The utility of LTE in achieving remarkable energy savings is validated by detailed performance evaluation.

2.1 EXISTING SYSTEM

Some distributed clone detection protocols have been proposed, such as¬ Randomized Efficient and Distributed protocol (RED)

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 17, March 2017

and Line-Select Multicast protocol (LSM). In most existing clone detection protocols, the required buffer storage size depends on the network node density, i.e., sensors need a large buffer to record the exchanged information among sensors in a high-density WSN, and thus the required buffer size scales with the network node density. Such requirement makes the existing protocols not so suitable for densely deployed WSNs.

2.1.1 DISADVANTAGES

- Most approaches mainly focus on improving clone detection probability without considering efficiency and balance of energy consumption in WSNs.
- Some sensors may use up their batteries 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 can improve the successful clone detection at the expense of energy consumption and memory storage, which may not be suitable for some sensor networks with limited energy resource and memory storage.

2.2 PROPOSED SYSTEM

Besides the clone detection probability, we also consider energy consumption and memory storage in the design of clone detection protocol, i.e., an energy- and memory-efficient distributed clone detection protocol with random witness selection scheme in WSNs. Proposed protocol is applicable to general densely deployed multi-hop¬ WSNs, where adversaries may compromise and clone sensor nodes to launch attacks. An energy-efficient ring based clone detection (ERCD) protocol to achieve high clone detection probability with random witness selection, while ensuring normal network operations with satisfactory network lifetime of WSNs. The ERCD protocol can be divided into two stages: witness selection and legitimacy verification.

2.2.1 BENFITS OF PROPOSED SYSTEM

- Energy efficient
- Memory efficient
- High network lifetime can be achieved

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 17, March 2017

3. SYSTEM MODEL AND PROBLEM DEFINITION

Different from wireless terminal devices, wireless sensors are usually of smaller size and lower price, and have limited battery and memory capacity. Therefore, the design criteria of clone detection protocols for sensor networks should not only guarantee the high performance of clone detection probability but also consider the energy and memory efficiency of sensors. To prolong the network lifetime, i.e., the 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.

Wireless sensors have been widely deployed for a variety of applications, ranging from environment monitoring to telemedicine and objects tracking, etc. 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. To allow efficient clone detection, usually, a set of nodes are selected, which are called witnesses, to help certify the legitimacy of the nodes in the network. The private information of the source node, i.e., identity and the location information are shared with witnesses at the stage of witness selection. When any of 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. To achieve successful clone detection, witness selection

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 17, March 2017

and legitimacy verification should fulfil two requirements:

1) Witnesses should be randomly selected; and

2) At least one of the witnesses can successfully receive all the verification message(s) for clone detection.

The first requirement is to make it difficult for malicious users eavesdrop the communication between the current source node and its witnesses, so that the malicious users cannot generate duplicate verification messages. The second requirement is to make sure that at least one of the witnesses can check the identity of the sensor nodes to determine whether there is a clone attack or not. To guarantee a high clone detection probability, i.e., the probability that clone attacks can be successfully detected, it is critical and challenging to fulfil these requirements in clone detection protocol design. Different from wireless terminal devices, wireless sensors are usually of smaller size and lower price, and have limited battery and memory capacity. Therefore, the design criteria of clone detection protocols for sensor networks should not only guarantee the high performance of clone detection probability but also consider the energy and memory efficiency of sensors. In the literature, some distributed clone detection protocols have been proposed, such as Randomized Efficient and Distributed protocol (RED) and LineSelect Multi-cast protocol (LSM). However, most approaches mainly focus on improving clone detection probability without considering efficiency and balance of energy consumption in WSNs. With such kind of approaches, some sensors may use up their batteries due to the unbalanced energy consumption, and dead sensors may cause network partition, which may further affect the normal operation of WSNs. [7] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC).

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 17, March 2017

ERCD protocol, which can achieve a high clone detection probability with little negative impact on network lifetime and limited requirement of buffer storage capacity. The ERCD protocol consists of two stages: 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. If witnesses receive the verification messages, all the messages will be forwarded to the witness header for legitimacy verification, where witness headers are nodes responsible for determining whether the source node is legitimacy or not by comparing the messages collected from all witnesses. If the received messages are different from existing record or the messages are expired, the witness header will report a clone attack to the sink to trigger a revocation procedure. Initially, the network region is virtually divided into h adjacent rings, where each ring has a sufficiently large number of sensor nodes to forward along the ring and the width of each ring is r. To simplify the description we use hop length to represent the minimal number of hops in the paper. Since it considers a densely deployed WSN, hop length of the network is the quotient of the distance from the sink to the sensor at the border of network region over the transmission range of each sensor, i.e., the distance of each hop refers to the transmission range of sensor nodes.

The ERCD protocol starts with a breadth-first search by the sink node to initiate the ring index, and all neighbouring sensors periodically exchange the relative location and ID information. After that, whenever a sensor node establishes a data transmission to others, it has to run the ERCD protocol, i.e., witness selection and legitimacy verification, to verify its legitimacy.

In witness selection, a ring index is randomly selected by the mapping function as the witness ring of node a. To help relieve the traffic load in hot spot, the area around the sink cannot be selected by the mapping function. After that, node a sends its private information to the node located in witness ring, and then the node forward the information along the witness ring to form a ring structure. In the legitimacy verification,

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 17, March 2017

a verification message of the source node is forwarded to its witnesses. The ring index of node a, denoted Oa, is compared with its witness ring index Oaw to determine the next forwarding node. If Oaw > Oa, the message will be forwarded to any node located in ring Oa + 1; otherwise, the message will be forwarded to any node in ring Oa 1. This step can forward the message toward the witness ring of node a. The ERCD protocol repeats above operations until a node, denoted b, located in the witness ring Oa w is reached. Node b stores the private information of node a and forwards the message to any node located in ring Oaw within its transmission range, denoted as c. Then, node c stores the information and forwards the message to the node d, where link (c,d) has longest projection on the extension line of the directional link from b to c. The procedure will be repeated until node b reappears in the transmission range. Therefore, the witnesses of node a have a ring structure, consisting of b,c,..b as shown in Fig. 1.

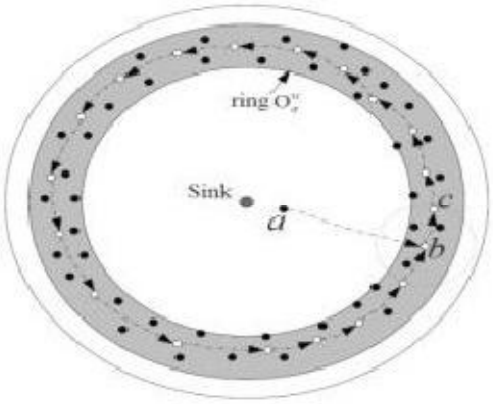

Fig.1 Ring structure of witness

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, i.e., the message will be broadcast in Oaw 1, Oaw and Oaw +1 as shown in Fig 2.

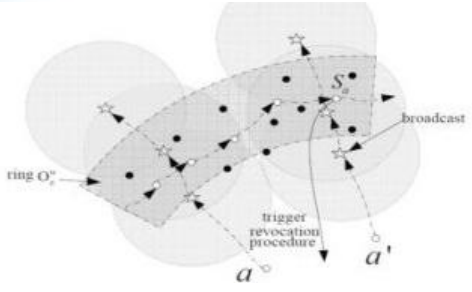

Fig.2 Legitimacy verification

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 17, March 2017

In Theorem 1, it proves that the three ring broadcasts can ensure the network security, i.e., the clone detection probability is one, under the assumption that all witnesses are trustful. To determine whether there exists a clone attack or not, all the verification messages received by witnesses are forwarded to the witness header along the same route in witness selection. The sensors nodes in the transmission route but not located in the witness ring are called the transmitters. The witness header of the source node a, denoted by Sa, is a sensor located in witness ring Oaw, meanwhile it is also in the communication range of the transmitter located in ring index Oaw or Oaw+1. The witness header Sa is randomly selected by the transmitter in the neighbouring witness ring, i.e., the ring of Oaw or Oaw + 1. If more than one copy or incorrect copies or expired copies are received by the witness header, the ERCD protocol will trigger a revocation procedure; if no copy is received from the source node due to packet loss or silent cloned node, transmissions from the source node will not be permitted.

3.1 MODULE DESCRIPTION

1. Legitimacy verification Module
2. Clone Detection Module

3.3.1 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.

3.3.2 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.

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 17, March 2017

4. CONCLUSION

The system proposed distributed energy efficient clone detection protocol with random witness selection. Specifically, it has proposed the ERCD protocol, which includes the witness selection and legitimacy verification stages. Both of the theoretical analysis and simulation results have demonstrated that the protocol can detect the clone attack with almost probability 1, since the witnesses of each sensor node is distributed in a ring structure which makes it easy be achieved by verification message. In addition, this protocol can achieve better network lifetime and total energy consumption with reasonable storage capacity of data buffer. This is because we take advantage of the location information by distributing the traffic load all over WSNs, such that the energy consumption and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended.

FUTURE ENHANCEMENT

In the future work, it may be considered different mobility patterns under various network scenarios.

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, Turin, IT, 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 Communications Magazine, vol. 49, no. 4, pp. 28–35, Apr. 2011.

[3] Christo Ananth, A.Nasrin Banu, M.Manju, S.Nilofer, S.Mageshwari, A.Peratchi Selvi, "Efficient Energy Management Routing in WSN", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume1, Issue 1, August 2015,pp:16-19

[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," Computer Networks, vol. 56, no. 7, pp. 1951–1967, May. 2012.

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 17, March 2017

[5] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sen-sor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941–954, Jul. 2010.

[6] P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized coun-termeasure against parasitic adversaries in wireless sensor networks,"

[7]Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[8] 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 Transactions on Vehicular Technology, vol. 61, no. 1, pp. 86–96, Jan. 2012.

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

[10] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 127–139, Jan. 2012.

[11] 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.