Clone Attack in Wireless Sensor Networks

Amanpreet Kaur[1] Dinesh Kumar[2]
[1]P.G. Student [2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]GZS, PTU Campus, Bathinda Punjab Technical University, Jalandhar

Abstract— The increasing growth of mobile sensor nodes technology and rising the deployment of them; these networks are faced with security challenges; specially clone nodes attack. In Mobile Wireless Sensor Network, the attacker can capture a node easily and compromise that sensor node and take out all the keying materials from that compromised node and make duplicate of them. These replica node attacks are hazardous because they permit the attacker to control the compromise of a few nodes to use control over much of the network .Then attacker use the replica node to insert fake data and disturb the whole operations in the network. In this paper an general review of the methodologies to identify or prevent such attacks has been presented.

Key words: Wireless Sensor Network, Clone Nodes, Energy Consumption, Clone Attack

I. Introduction

The accelerating development of WSNs in different locations, such as medical and military areas, due to the reasonably priced, self-organizing and not requiring constant administration of sensor nodes is increasing. But concerning the inexpensiveness of sensor nodes, need of physical shield layer on these nodes and using them in adversary environment without security, usually these networks are at the disclosure of different internal and external attacks. Due to the limited energy and memory sources of these sensor nodes, the security challenges in these networks are meeting more complexity as contrasted to other mobile telecommunication networks. These complexities are increased if the sensor nodes have mobility.

Regarding the organization and design of WSNs, different attacks are introduced. Different attacks included are DDos attack, clone attack and Sybil attack. In DDos attack, the attack is performed with the aim to make network resources unavailable and generally involve a large number of machines that target the same purpose interrupting or suspending the services it offers. The principle on which the attack approach is based is the dispersion of the resources available to the targets that are flooded by reasonable traffic that are not able to process. The consuming of the resources of final target may usually causes the decelerate in services provided or even total blockage of the same. In Sybil attack a wicked node illegally declares multiple identities. This attack can extremely interrupt various operations of the networks such as voting, data aggregation, fair resource allocation mechanism, misbehaviour detection and routing methods etc. In clone attack a challenger can physically capture some of the nodes, reprogram it, then can replicate them in a large number of clones, control can be effortlessly taking over the network. In this paper various techniques related to detect the clone attacks was studied and presented here.

II. Related work

In [1], authors projected a location-aware clone detection protocol, which guarantee victorious clone attack detection and have a little negative impact on the network lifetime. Particularly, they use the location information of sensors and randomly select witness nodes located in a ring area to confirm the privacy of sensors and to detect clone attacks. The ring structure made possible energy efficient data forwarding beside the path towards the witnesses and the sink, and the passage load is distributed across the network that recovers the network lifetime notably. Theoretical analysis and simulation results display that the proposed protocol can approach 100% clone detection probability with trustful witnesses. Moreover, their proposed protocol can considerably progress the network duration, compared with the existing approach.

In [2], authors projected the time and location based clone detection technique. In Location Claim technique that is an efficient clone detection protocol works on grid deployment. It can identify the clone nodes by sending each node's location claim (location and ID) to other nodes in a predestined area. The pointless forwarding of location claim among the sensor nodes will raise the claim storeroom, contact and computation overhead. Hence in the proposed study the technique is developed to defeat these problems by making the deployment location more precise. This is attained for all sensor nodes by assigning the time interval. Hence in this proposed work, an erroneously installed node which is marked as untrusted node finishes the neighbour discovery earlier than the time interval. Therefore it can be mentioned as trusted node.

In [3], authors planned a solution in networks of mobile devices carried by individuals - collected by nodes that can communicate by short-range technology like Wi-Fi or bluetooth, and links disappear and appear according to social relationships among users. Their idea is to utilize social physical contacts, firmly collected by wireless personal smart phones, as a biometric means to verify the owner of the device and detect the clone attack. They introduced two techniques: Personal Marks and Community Certificates. Personal Marks is a easy cryptographic protocol that works fine when the adversary is an insider, a wicked node in the network that tries to use the stolen testimonials in the social community of the original device that has been replicated. Community Certificates works fit when the adversary is an outsider, a node that has the aim of using the stolen credentials when cooperate with other nodes that are far in the social network from the original device. When united, these mechanisms provide an excellent security against this very strong attack.

In [4], authors proposed a hybrid (centralized and distributed) node replication attack finding technique for mobile WSN, that works based on Danger Theory in human immune system. As described in Danger Theory, the planned method consists of two main security approaches that are attack detection and security control. These approaches presented a multi-level detection that is not only accountable to identify but also to verify the survival of clone nodes in the network. Performance appraisal shows the efficiency (in terms of true and false positives) of the proposed detection technique in detecting clone nodes in mobile WSN environment.

In [5], authors proposed a clone detection technique and offer several aids: first authors set up two novel practical adversary models, the vanishing and the persistant adversary, categorized by different compromising ability. Then the Authors put forward two distributed, efficient, and supportive protocols to detect replicas: History Information exchange Protocol (HIP) and its optimized version protocol (HOP). Both protocols that are HIP and HOP control just local (one-hop) communications and node mobility, and vary for the required amount of computation. Authors revised their actions against the introduced types of attacker, considering two different models of mobility and comparing their solutions against the state of the art. Investigation and simulation results show that their solutions are effective and proficient, providing high detection rate, while having limited overhead.

In [6], authors projected a social closeness based technique in a mobile healthcare disease control system to identify any clone attack that may be initiated to interrupt the normal actions of the system. Their social closeness based technique develops the social relationships between users for clone attack detection. Particularly, they described a new metric called community betweeness, which regards as mobile users' community data. They analyze that the worth of this metric changes considerably under the clone attack, which is appropriate to be used for clone attack detection. They obtained both analytical and training based methodologies to define the threshold setting of the community betweenness for robust clone attack detection.

In [7], authors projected a new mechanism for detecting clone attacks in sensor networks, which computes for each sensor a social fingerprint by mining the neighbourhood features, and confirming the legitimacy of the instigator for each message by ensuring the enclosed fingerprint. The fingerprint creation is works on the superimposed s-disjunct code that acquires a very light communication and computation overhead. The fingerprint verification is accomplished at both the base station and the neighbouring sensors, which certifies a high detection probability. The security and performance study specify that their algorithm can recognize clone attacks with a high detection probability at the cost of a low communication/computation/ storage overhead.

In [8], authors developed methods for such an attack when there are multiple attackers in a network, and originate multi-player games to model the non-cooperative strategic activities between the attackers and the network. They deemed two cases: a static case where the attackers' node capture charges are time-invariant and the network's clone detection/revocation rate is a linear function of the state, and a dynamic case where the rates are general functions of time. They distinguished Nash equilibrium solutions for both cases and developed equilibrium strategies for the players. In the static case, they studied both the single-attacker and the multi-attacker games within an optimization framework, provide conditions for the survival of Nash equilibria and distinguish them in closed forms. In the dynamic case, they studied the underlying multi-person differential game under an open-loop information structure and offered a set of conditions to distinguish the open-loop Nash equilibrium. They showed the equality of the Nash equilibrium for the multi-person game to the saddle-point equilibrium between the network and the attackers as a team.

In [9], authors projected a novel method to detect the node clone attack in WSN by channel identification characteristic is existed, in which the clone nodes are notabled by the channel replies between nodes. The proposed method attempted at reaching fast detection and minimising the data communication cost by taking advantage of temporal and spatial uniqueness in physical layer channel reaction. In comparison to previous solutions, the proposed methods feature nearly-perfect flexibility to node clone attack with low transmission and computation costs, low requirements of memory and high detection chances.

In [10] authors proposed a novel distributed solution (RAND) for the detection of replication node attack in static WSNs that combines random walks with network division and operates in two stages. In the first stage called network configuration stage, the whole network is divided into varied areas. In the second stage called replica detection stage, the clone is detected by following a claimer-reporter-witness framework and a random walk is engaged within each area for the selection of witness nodes. Simulation results show that this scheme outperforms the existing witness node based strategies with reasonable communication and memory overhead.

In [11], authors projected a technique for detection of distributed sensor cloning attack by using of zero knowledge protocol (ZKP) for confirming the accuracy of the sender sensor nodes. The cloning attack is tackled by attaching a unique fingerprint to each node that relies on itself and the set of neighbouring nodes. The fingerprint is attached with every message that a sensor node sends. The ZKP is used to certify non transmission of vital cryptographic information in the wireless network in order to avoid man-in-the middle (MITM) attack and replay attack.

In [12], authors planned an inventive randomly directed exploration protocol to identify the node clone. Each node requires to only knowing its neighbours' information, and then joined to forward claiming messages, demanding to find out clone. The specific routing protocols or infrastructures are not demanded in the proposed protocol. Consequently, it is highly practical in the common sensor network purposes. In addition, the requirement of memory of the protocol is almost best possible. Furthermore, the protocol uses relatively low communication overload, which is not mediocre to any previous schemes.

Acknowledgment

The paper has been written with the kind guidance, assistance and active support of my department who have helped me in this effort. I would like to thank all the individuals whose encouragement and support has made the completion of this work feasible.

REFERENCES

[1] Zhongming Zheng, Anfeng Liu, Cai, L.X.; Zhigang Chen, Xuemin Shen, “ERCD: An energy-efficient clone detection protocol in WSNs”, Proceedings IEEE INFOCOM, 2013

[2] Sivaraj, R.; Thangarajan, R “Location and Time Based Clone Detection in Wireless Sensor Networks," Fourth International Conference on Communication Systems and Network Technologies (CSNT), 2014

[3] Barbera, M.V.; Mei, A: Personal Marks and Community Certificates: Detecting Clones in Wireless Mobile Social Networks”. IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2012.

[4] Shaukat, H.R.; Hashim, F.; Sali, “Danger theory based node replication attacks detection in mobile wireless sensor network," IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), 2014.

[5] M. Contia, R. Di Pietrob, A. Spognardic, “Clone wars: Distributed detection of Clone attacks in mobile WSNs.” Journal of Computer and System Science, 654-669, 2014

[6] Yanzhi Ren; Yingying Chen; Mooi Choo Chuah “Social closeness based clone attack detection for mobile healthcare system”. IEEE 9th International Conference on Mobile Adhoc and Sensor Systems (MASS), 2012.

[7] Kai Xing; Fang Liu; Xiuzhen Cheng; Du, D.H.C. “Real-Time Detection of Clone Attacks in Wireless Sensor Networks”. The 28th International Conference on Distributed Computing Systems, 2008. ICDCS '08.

[8] Quanyan Zhu; Bushnell, L.; Basar, T “Game-theoretic analysis of node capture and cloning attack with multiple attackers in wireless sensor networks”. IEEE 51st Annual Conference on Decision and Control (CDC), 2012.

[9] Wen, H.; Luo, J.; Zhou, L “Lightweight and effective detection scheme for node clone attack in wireless sensor networks” IET Wireless Sensor Systems.

[10] Khan, W.Z.; Aalsalem, M.Y.; Saad, N.M.; Yang Xaing; Luan, T.H, “ Detecting replicated nodes in Wireless Sensor Networks using random walks and network division,” IEEE Wireless Communications and Networking Conference (WCNC), 2014

[11] Udgata, S.K.; Mubeen, A.; Sabat, S.L. “Wireless Sensor Network Security Model using Zero Knowledge Protocol”. IEEE International Conference on Communications (ICC), 2011.

[12] Zhijun Li; Guang Gong “Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks”. IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, 2009. MASS '09.