iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 Issue: III Month of publication: March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3319

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Survey on Identification of Clone Node in WSN using Red Black Tree Mechanism

N. Sankar Adhithya[1], G. Senthil Raghavan[2], V. Surya[3]
[1, 2, 3]Department of computer science and engineering Ap. N.S usha

Abstract: Wireless sensor network is usually deployed in environments where there are many attacks and an opponent can physically capture some of the sensors, build clones with the same identity as the captured sensors, and place these clones in the network's strategic positions for further malicious activities, these types of attacks are called clone attacks, and they are very serious. To detect such attacks, researchers proposed different techniques. In this paper, by assigning a color to clone detection, we present the RED BLACK tree detection mechanism. For example, detecting an attack by a previous technique will be difficult.

I. INTRODUCTION

Wireless Sensor Network (WSN) consists of a series of low - cost, small - resource sensor nodes. Stationary and mobile networks are available. Sensors move in mobile networks, while they remain in stationary networks. We look at stationary networks in what follows. Such networks are often used in inaccessible areas to collect different information, such as monitoring the environment and tracking objects. Since sensors are not normally equipped with manipulator-resistant hardware, sensor networks are vulnerable to attacking node clones. Since all clones have valid credentials, they can act as normal sensors as well as devious attackers. Clones can also launch insider attacks that are potentially baleful for the network's functionality.

A. Related Works

1) Becher, A., Benenson, Z., & Dornseif, M. (2006, April). Most Wireless Sensor Networks (WSN) security protocol assumes that the attacker can gain full control of a sensor node by capturing a node (direct attack). But the amount of effort an attacker has to make in a node capture attack is unknown so far. We evaluate various physical attacks against node hardware in our project. By providing detailed knowledge of the effort required for physical attacks to adjust security protocols in WSNs, they provide optimal protection at minimal costs.
2) Rasmussen, K. B., & Capkun, S. (2007, September). We show the feasibility of wireless sensor nodes fingerprinting (Chipcon 1000 radio, 433MHz). We show that a receiver can use this type of device to create device radio fingerprints and then identify the origins of messages exchanged between devices, even if the content of messages and device identifiers is hidden. We propose two new mechanisms to detect wormholes in sensor networks and further analyze the impact of device fingerprinting on sensor network protocol security.
3) Xing, K., Liu, F., Cheng, X., & Du, D. H. (2008, June). A major problem with the security of the sensor network is the sensors ' sensitivity to physical capture attacks. The opponent can easily start clone attacks once a sensor node is compromised by replicating the affected node, distributing clone nodes across the network, and initializing a variety of insider attacks. Previous work on clone attacks has suffered either from high overhead communication / storage or poor detection accuracy. This paper proposes a new scheme for detecting clone attacks in a sensor network, calculating a social fingerprint for each sensor by extracting and identifying neighborhood characteristics, and also verifying the originator's legitimacy for each message by checking the fingerprint included. Fingerprint generation is based on the superimposed s - disjunction code, resulting in very light communication and overhead computing. The verification of fingerprints is performed at both the base station and the adjacent sensors, ensuring a high detection probability. The safety and performance analysis shows that at the cost of low overhead computing / communication / storage, our algorithm can identify clone attacks with a high probability of detection. Our system is the first to detect clone attacks effectively and efficiently in sensor networks to the best of our knowledge.
4) George, N., & Parani, T. K. (2014). Wireless sensor networks are made up of hundreds to thousands of sensor nodes and are widely used in civil and security applications. Node clone attack is one of the serious physical attacks facing a wireless sensor network. The two protocols for the detection of node clones are introduced via a distributed hash table and random exploration to detect node clones. The former is based on a hash table and exploration to detect node clones is randomly directed. The former is based on a hash table value that is already distributed and provides a key facility to detect node clones, such as

checking and caching. Later one uses for border determination probabilistic directed forwarding techniques. The simulation result for communication costs, storage consumption and probability of detection is performed using NS2 and randomly directed exploration is considered to be the best with low cost communication and storage consumption and a good probability of detection.

5) Choi, H., Zhu, S., & La Porta, T. F. (2007, September). Capture and compromise sensor nodes deployed in hostile environments are vulnerable. An attacker can collect, clone, and deploy private information from these sensor nodes in order to initiate a variety of network insider attacks. This attack is widely referred to as an attack by clones.There are currently not only very few defenses against these types of clone attacks, but they also suffer from selective detection interruptions and high overhead (computing and memory). We propose in this paper an efficient and effective scheme, called SET, to detect clone attacks of this kind. SET's main ideas are to detect clones from exclusive network subsets by computing set operations, intersection and union. First, SET securely forms distributed exclusive unit subsets among the networks one-hop neighbours. This secure sub-set formation also authenticates the membership of the sub-set nodes. A SET uses a tree structure to calculate unchecked set operations and integrate interleaved authentication during transmission to avoid unauthorized forgery of sub - set information. Randomization is used to make an adversary unpredictable for exclusive subsets and tree formation. By analyzing the likelihood that an opponent can effectively block the set operations, we show the reliability and resilience of SET. Performance analysis and simulations also show that the proposed scheme is more efficient than the existing schemes from the point of view of communication and memory costs.

6) Ho, J. W., Liu, D., Wright, M., & Das, S. K. (2009, March). A number of protocols have been developed to mitigate the threat to an attacker's wireless sensor networks that find nodes, compromise them and use these nodes to escape or undermine the network's operation. However, the replica node, in which the attacker compromise a node, extracts its key materials and produces a large number of replicas that can be spread across the network, is a more dangerous threat received less attention. This attack allows the opponent to leverage a single node compromise to create widespread network effects. We propose a distributed detection mechanism to find and revoke replicas in order to defend against these attacks. Our programs are based on the assumption that for many deployment scenarios nodes are deployed in a group that is realistic. Our systems use knowledge of group deployment to perform replica detection in a distributed, efficient and secure manner. In the simulation, our systems achieve robust and efficient replication detection with significantly lower overheads for computational communication and storage than previous works.

7) Zhu, W. T., Zhou, J., Deng, R. H., & Bao, F. (2012). Wireless sensor networks are made from a variety of minimal efforts, low-control sensor hubs. It is used through remote connections for short term communication. Sensors are deeply transmitted to collect and transmit information about the physical world to one or two goals called sinks. The attacker can catch investigation hubs and repeat them with little effort. These copies can corrupt network data or disconnect significant parts of the network in different areas of the system. These copies can corrupt network data or disconnect significant parts of the network in different areas of the system. Once the hub is caught and keys are collected, etc. The attacks can reinvent it and duplicate the hub, bearing in mind that the ultimate goal is to escape the messages transmitted. In distributed sensor networks, the proposed system is used to detect the replicated node.

8) Mishra, B., & Singh, Y. (2015, December). We analyzed the detection techniques in wireless sensor networks for distributed node clones in this paper. Although many literature protocols are proposed for the detection of node clones, we discussed some effective protocols such as LSM and RED in the category of node clone detection based on witnesses. We analyzed the LSM, RED and proposed protocol detection level, memory and energy overhead. We presented an approach to optimizing the detection of distributed node clones based on witnesses. We have provided the mathematical and simulation results for the various WSN parameters for the validation of the proposed protocol performance.

9) Autkar, S. V., Dhage, M. R., & Bholane, S. P. (2015, January). Wireless sensor networks consist of a sensor node placed in a harsh and hostile environment in which an opponent can capture, replicate and use the nodes for their own purposes. If clone nodes remain undetected, vulnerability of attack may disrupt the network function. False data can therefore be injected or legitimate data can be extracted. The fundamental problem in WSN is detecting the node clone attack to preserve a security goal. Centralized methods have been proposed to detect clones consisting of a single point of failure. Distributed protocols are therefore used to detect clone nodes where there is no central authority and detection is the responsibility of each node. This paper presents different existing distributed techniques based on witnesses for the detection of node clones in the network.

10) Zheng, Z., Liu, A., Cai, L. X., Chen, Z., & Shen, X. S. (2013, April). Wireless sensor networks (WSNs) play a growing role in a wide range of applications, from hostile environment surveillance to telemedicine services. However, the hardware and cost constraints of sensor nodes make sensors susceptible to clone attacks and pose major challenges in the design and deployment of WSN energy efficiency. We propose a location-conscious clone detection in this paper and have little negative impact on the life of the network. We use the sensor location information to detect clone attacks and specifically select witness nodes in a ring area to verify the sensor privacy. The ring structure facilitates the transmission of energy-efficient data to witnesses and the sink along the path and distribution of traffic load across the network, significantly improving network life. Theoretical results of analysis and simulation show that the proposed protocol can approach the probability of 100% clone detection with a trustworthy witness. We also extend the work by studying clone detection performance with trustworthy UN witnesses and show that when 10 percent of witnesses are compromised, the probability of clone detection remains close to 98 percent. Furthermore, our proposed protocol can significantly improve the network's life compared to the existing approach.

11) Sivaraj, R., & Thangarajan, R. (2014, April). Wireless sensor networks consists of several sensor nodes deployed in an unattended environment to monitor and record environmental changes. The attacker can capture and compromise sensor nodes that can communicate via a wireless channel. An opponent can replicate a few sensor nodes after such a compromise and insert an arbitrary number of replicas into the network field to undermine the operation of the network. As a framework for maximizing the security and life of wireless sensor networks, multiple protocols for clone detection have been proposed. These are based on types of device nodes, deployment strategies, methods of detection and ranges of detection, and attempt to mitigate the threat to wireless sensor networks. Location Claim Approach is an effective grid deployment - based clone detection protocol. Clone nodes can be detected by sending to other nodes in predetermined areas each device location request (location and ID). However, there are some limitations to the current study. The unnecessary location claim transmission between the sensor nodes increases the claim's overhead storage, communication, and computing. Therefore, in the proposed system, the methodology is developed to overcome these problems by making the deployment location more accurate. This is achieved by assigning the time interval to all sensor nodes. Therefore, a mistakenly deployed node marked as an untrusted node completes the neighbor's discovery before the time interval in this proposed work. It can therefore be noticed as a trusted node. Finally, the total energy consumed by the method proposed consumes less energy.

12) Grewal, R., Kaur, J., & Saini, K. S. (2015, June). Because of the open use of sensor nodes in a hostile environment and the lack of physical shielding, sensor networks are exposed to various types of physical threats, including clone attacks, in which an opponent physically compromises the node, extracts all credentials such as keys, identity and stored codes, replicates the hardware with the captured information and introduces them at specified locations. The detection of replicas has become an important and challenging security issue. These papers examine existing clone attack detection schemes. To conclude the paper, all existing literature techniques are compared.

13) Yu, C. M., Lu, C. S., & Kuo, S. Y. (2012, March). Because of clones impact on network operations such as routing, data collection, key distribution, etc., clone detection to detect the clone node with all the credentials of legitimate sensor nodes is of great importance for sensor networks. We are proposing a new method of clone detection, called CSI, based on a state-of - the-art, compressed sensing technique. Not only is the design philosophy fundamentally different from the existing system and has the lowest communication cost between all methods of detection. Numerical simulations and analyzes demonstrate CSI's performance and safety.

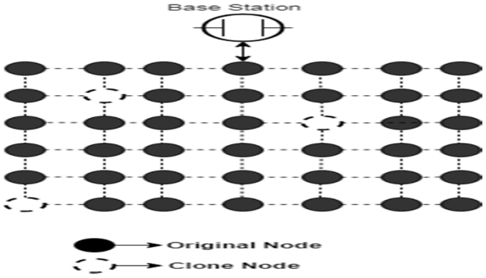
14) Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks Because of the poor physical protection of sensor devices, an opponent can generally capture a small number of sensor devices in the network. An opponent can use the credentials of a compromised node in a replication attack on the sensor device to surreptitiously introduce the clone of that node into the network. These replicas can be used to launch a variety of attacks that undermine many sensor applications and protocols without an effective and efficient detection mechanism. In this paper, we are presenting a new distributed approach for the detection of clone nodes called Localized Multicast. The efficiency and safety of our method is theoretically and cumulatively assessed. Parno et al. provides our results compared to previous distributed algorithms, and the Localized Multicast is more efficient in terms of communication and memory costs in large sensor networks, while at the same time achieving a higher probability of detecting clone nodes.

15) Published in: 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) .The sensor nodes in the Wireless Sensor Network transmit critical information over the network ; Security services such as authentication and wise key setting between sensor nodes and mobile sinks are therefore important. However, the issue of authentication and pairwise key establishment in sensor networks with MSs is still not solved in the face of mobile sink replication attacks. An enemy can easily obtain a large number of keys for the basic probabilistic and q - composite key of pre - distribution modules by capturing a small fraction of the network sensor device, enabling the attacker to control the entire network using a replicated mobile sink, which is preloaded with some compromised keys to authenticate and then initiate data communication with an authentication device. To solve this problem, a general framework has been developed that allows the use of any pair of wise key pre - distribution modules as its basic component for authentication and pairing between sensor nodes and Mss. The new framework needs two separate key pools, one for the network's mobile sink and the other for the establishment of a pair of key keys between the sensor nodes.

B. *Proposed System*

In this proposed system we using red black tree mechanism to detect the identification of clone node. A red–black tree is a kind of self-balancing binary search tree. Each node of the binary tree has an extra bit, and that bit is often interpreted as the color of the node. These color bits are used to ensure the tree remains approximately balanced during insertions and deletions. We assigning color for every node. In the position of red color adjacent node has to be black. If there any color mismatching and there is an clone detection and it directly indicated to the base station.

Architecture Diagram



II. CONCLUSION

This paper deals with the existing detection systems used to mitigate clone attacks in WSN. Physical attacks on the hardware of the node sensors provide optimal protection at minimal costs. Since each nodes are given a color which is different from the adjacent node, we can easily detect the clone node and it is indicated to the base station.

REFERENCES

[1] Becher, A., Benenson, Z., & Dornseif, M. (2006, April). Tampering with motes: Real-world physical attacks on wireless sensor network

[2] Rasmussen, K. B., & Capkun, S. (2007, September). Implications of radio fingerprinting on the security of sensor networks. In security and Privacy in Communication Networks and the Workshops, 2007. Secure Comm. 2007. Third International Conference on (pp. 331-340). IEEE

[3] Xing, K., Liu, F., Cheng, X., & Du, D. H. (2008, June). Real-time detection of clone attacks in wireless sensors network. In Distributed Computing Systems, 2008. ICDCS'08. The 28th International Conference on (pp. 3-10). IEEE.

[4] George, N., & Parani, T. K. (2014). Detection of node clones in wireless sensor network using detection protocols. ArXiv preprint arXiv: 1403.2548.

[5] Choi, H., Zhu, S., & La Porta, T. F. (2007, September). SET: Detecting node clones in sensor networks. In Security and Privacy in Communications Network and the Workshops, 2007. Secure Comm. 2007. Third International Conference on (pp. 341-350). IEEE.

[6] Ho, J. W., Liu, D., Wright, M., & Das, S. K. (2009, March). Distributed detection of replica with deployment knowledge in wireless sensor networks. In Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on (pp. 1-6). IEEE

[7] Zhu, W. T., Zhou, J., Deng, R. H., & Bao, F. (2012). Detecting node replication attacks in wireless sensor networks: a survey. Journal of Network and Computer Applications, 35(3), 1022-1034.

[8] Mishra, B., & Singh, Y. (2015, December). An approach towards the optimization of witness based node clone attack. In Image Information Processing (ICIIP), 2015 Third International Conference on (pp. 506-510). IEEE

[9] Autkar, S. V., Dhage, M. R., & Bholane, S. P. (2015, January). A survey on distributed techniques for detection of node clones in Wireless Sensor Network. In Pervasive Computing (ICPC), 2015 International Conference on (pp. 1-4). IEEE.

[10] Zheng, Z., Liu, A., Cai, L. X., Chen, Z., & Shen, X. S. (2013, April). ERCD: An energy-efficient clone detection protocol in WSNs. In INFOCOM, 2013 Proceedings IEEE (pp. 2436-2444). IEEE.

[11] Sivaraj, R., & Thangarajan, R. (2014, April). Location and Time based clones detection in wireless sensor networks. In Communication Systems and Networks Technologies (CSNT), 2014 Fourth International Conference on (pp. 133-137). IEEE.

[12] Grewal, R., Kaur, J., & Saini, K. S. (2015, June). A survey on proficient techniques to mitigate Clone attacks in wireless sensor networks. In Advance Computing Conference (IACC), 2015 IEE International (pp. 1148-1152). IEEE.

[13] Yu, C. M., Lu, C. S., & Kuo, S. Y. (2012, March). CSI: compressed sensing-based clone identification in sensor networks. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on (pp. 290-295). IEEE.

[14] Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks Published in: IEEE Transactions on Mobile Computing (Volume: 9, Issue: 7, July 2010) Page(s): 913 - 926 Date of Publication: 18 March 2010 ISSN Information

[15] Published in: 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) Active key management scheme to avoid clone attack in wireless sensor network Publisher: IEEE Conference Location: Tiruchengode, India