ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Survey on: Low-Priced and Energy-Efficient Detection of Replicas for Wireless Sensor Networks

Chavan Laxman N., Prof. Bere S. S.

P.G. Scholar, Dept. of Information Technology, DGOI, FOE, Bhigwan, Savitribai Phule University of Pune, Pune, India

Professor, Dept. of Computer Engineering, DGOI, FOE, Bhigwan, Savitribai Phule University of Pune, Pune, India

ABSTRACT: The one of most challenging problem is the replica attack in static wireless sensor network. Also every sensor nodes are physically captured. These nodes are reprogramming and replicated in large number of replicas. Which may dynamically occupy the network Thus far different ways to detect the replicas? Most of the sensor nodes required high costs hardware like as:"Global Positioning System". In general, Sensor nodes are low price as compared to GPS hardware. On this paper, we proposed "Low Priced and Energy-Efficient Detection of Replicas in Static Wireless Sensor Network". On this proposed solution not required any internal hardware such as: GPS. Good performances as compared to exiting system. We show that the proposed solution saves the lot of energy than exiting system.

KEYWORDS: Security and protection, authentication, network protocols, ubiquitous computing

I.INTRODUCTION

Wireless sensor network are provides two different technologies such as: computation and communication. It consists of large number of sensing devices also support for: Physically and Environmental conditions like: Humidity, Temperature, Pressure, Sound etc.Data collected by sensing devices and also transmitted to the destination .It also known as base station or sink. WSN's have various security challenges as compared to traditional network. The sensor nodes generally support for tamper resistances behind the hardware. It also spread in insecure environments. where they are not grunted to capture and compromise attack. These replicas can be used for various launch stealth attack depending on the attackers motives. The such as listen secretly to private on network communication or controlling the source areas. This type of attack is also known as "Replica attack".

Accordingly, without using hardware like: GPS, we design low price replica detection solution for static wireless sensor network by using "Bloom Filter" and "Sequential delivery algorithm". Neighbouring nodes IDs also presented with constant size by using Bloom Filter. "Bloom Filter Output" (BFO): uses for proof. The in this methods slowly increase traffic between the neighbouring node and randomly selected nodes ,then exiting system generates heavy traffic by transmitting proofs form the starting. The entire result shows that the proposed solution is more energy efficient than exiting system.The contribution of purposed solution as follows:low price solution: 1) The proposed solution also reduces the cost of building wireless Sensor Network replica detection. 2) Efficient - energy detection: energy efficiency is important in wireless sensor network. we consider node in environment are often non rechargeable and hence availability depends on energy efficiency support for large scale.[1]

Replica Attack and Detection Scenario:

An attacker captures one or more nodes deployed in the network and then obtains secret information from them. Next, the attacker makes multiple replicas by using this information and then deploys them into targeted areas. Here, the neighboring nodes recognize replicas as newly deployed nodes. For obtaining useful information from the neighboring nodes in the target areas or controlling the neighboring nodes, replicas should prove that they are legitimate nodes with valid secret information. However, since replicas already know the secret information, they can prove it to the neighboring nodes without difficulty. Hence, before proving the legitimacy, all newly inserted nodes (some of which may be replicas) must pass the replica detection test more than once.

DOI: 10.15680/IJIRCCE.2015. 0311238

II.LITERATURE SURVEY

In the past decade, internet of things (IoT) has been a focus of research. Security and privacy are the key issues for IoT applications, and still face some enormous challenges.[1] In order to facilitate this emerging domain, we in brief review the research progress of IoT, and pay attention to the security. By means of deeply analysing the security architecture and features, the security requirements are given. On the basis of these, we discuss the research status of key technologies including encryption mechanism, communication security, protecting sensor data and cryptographic algorithms, and briefly outline the challenges.[1]

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, analyse 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.[3] Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighbourhood 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 nodes can be captured, replicated and re-inserted by an adversary.[3]

Wireless Sensor Networks (WSNs) are often deployed in hostile environments where an adversary can physically capture some of the nodes, first can reprogram, and then, can replicate them in a large number of clones, easily taking control over the network.[4] A few distributed solutions to address this fundamental problem have been recently proposed. However, these solutions are not satisfactory. First, they are energy and memory demanding: A serious drawback for any protocol to be used in the WSN-resource-constrained environment. Further, they are vulnerable to the specific adversary models introduced in this paper. The contributions of this work are threefold. First, we analyze the desirable properties of a distributed mechanism for the detection of node replication attacks. Second, we show that the known solutions for this problem do not completely meet our requirements. Third, we propose a new self-healing, Randomized, Efficient, and Distributed (RED) protocol for the detection of node replication attacks, and we show that it satisfies the introduced requirements. Finally, extensive simulations show that our protocol is highly efficient in communication, memory, and computation; is much more effective than competing solutions in the literature; and is resistant to the new kind of attacks introduced in this paper, while other solutions are not.[4]

Sensor nodes that are deployed in hostile environments are vulnerable to capture and compromise. An adversary may obtain private information from these sensors, clone and intelligently deploy them in the network to launch a variety of insider attacks.[6] This attack process is broadly termed as a clone attack. Currently, the defences against clone attacks are not only very few, but also suffer from selective interruption of detection and high overhead (computation and memory). In this paper, we propose a new effective and efficient scheme, called SET, to detect such clone attacks. The key idea of SET is to detect clones by computing set operations (intersection and union) of exclusive subsets in the network. First, SET securely forms exclusive unit subsets among one-hop neighbours in the network in a distributed way. This secure subset formation also provides the authentication of nodes' subset membership. SET then employs a tree structure to compute non-overlapped set operations and integrates interleaved authentication to prevent unauthorized falsification of subset information during forwarding. Randomization is used to further make the exclusive subset and tree formation unpredictable to an adversary. We show the reliability and resilience of SET by analysing the probability that an adversary may effectively obstruct the set operations. Performance analysis and simulations also demonstrate that the proposed scheme is more efficient than existing schemes from both communication and memory cost standpoints.[6]

Wireless sensor networks are vulnerable to the node clone attack because of low-cost, resource-constrained sensor nodes, and uncontrolled environments where they are left unattended.[7] Several distributed protocols have been proposed for detecting clone. However, some protocols rely on an implicit assumption that every node is aware of all other nodes' existence; other protocols using an geographic hash table require that nodes know the general network deployment graph. Those assumptions hardly hold for many sensor networks. In this paper, we present a novel node clone detection protocol based on Distributed Hash Table (DHT). DHT provides good distributed properties and our protocol is practical for every kind of sensor networks. We analyse the protocol performance theoretically. Moreover, we implement our protocol in the OMNeT++ simulation framework. The extensive simulation results show that our protocol can detect clone efficiently and holds strong resistance against adversaries.[7]

Existing System:

- WSNs have encountered a variety of security challenges, as compared to traditional networks, because the sensor nodes generally lack hardware support for tamper-resistance and are often deployed in physically insecure environments, where they are vulnerable to capture and compromise by attackers. A harmful consequence of a node compromise attack is that once an attacker has acquired the credentials of a sensor, he/she can fabricate replicas with these credentials and then surreptitiously insert them at selected target Positions within the network.

Disadvantages of Existing System:

- Replicas can be used to launch various stealth attacks depending on the attacker's motives, such as eavesdropping on network communications or control-ling the target areas. This type of attack, which is called a replica attack.

III.PROPOSED ALGORITHM

System Architecture:

Sensor networks are usually designed and deployed for a specific application. They are scalable with a minimal effort. Network topology changes frequently in WSN due to energy depletion, channel fading, node failure and damage. Sensor nodes are self-configurable and they are densely deployed in the target area. Battery is the only source of energy for most of the sensing devices. Most of the applications of WSN are data centric and the data-flows within the network obey many-to-one traffic pattern. Due to higher node density, data redundancy may exist in the network.

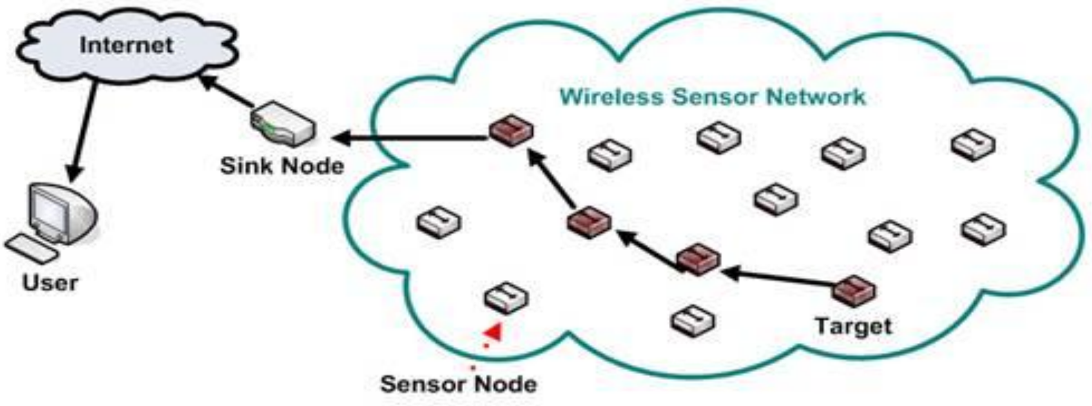

Figure 1: System Architecture of Wireless Sensor Network

DOI: 10.15680/IJIRCCE.2015. 0311238

MODULES:

1. **Node Formation:**
Neighbouring node IDs are presented with a constant size using a Bloom filter. The Bloom filter output (BFO) is used as a proof. A newly deployed node generates different proofs according to the collected neighboring nodes ID’s until collecting the entire neighboring node ID’s. The proofs are delivered to a randomly selected node in the networkATmega168 Microcontroller.[6]

2. **Find Attacker:**
With regard to this attack, it is assumed that an attacker captures only a small fraction of nodes in the network because capturing a large fraction may not require replicas any more, and it may be more costly and detectable. It is reasonable to assume that an attacker captures only a few nodes and obtains secret information from the captured nodes.

3. **Replica Attack and Detection Using Bloom Filter:**
An attacker captures one or more nodes deployed in the network and then obtains secret information from them. Next, the attacker makes multiple replicas by using this information and then deploys them into targeted areas. Here, the neighbouring nodes recognize replicasas why deployed nodes. For obtaining useful information from the neighboring nodes in the target areas.

4. **Validation of Node**
The RDB-R consists of three stages: proof generation, proof delivery, and proof validation. Henceforth, we explain the three stages with new deployment node A, the neighboring node C, and the witness node U. In the First Stage a proof for identifying a replica is created and updated in a newly added node.

5. **Duplicate Node Detection :**
The nodes which are captured by an adversary can compromise the sensor nodes and make many replicas of them. These compromised nodes all have the same ID are present in the network [6]. To understand the dangers of node compromise, we must first define what we mean by node compromise. Node compromise occurs when an attacker, though some subvert means, gains control of a node in the network after deployment. Once in control of that node, the attacker can alter the node to listen to information in the network, input malicious data, cause DOS, black hole, or any one of a myriad of attacks on the network. The attacker may also simply extract information vital to the network’s security such as routing protocols.

6. **Randomized Multi cast:**
Same as the previous approach, but the neighbors probabilistically send the location information to randomly selected witnesses. If there is a replicated node, any one of this witness may receive the different location claims with same ID and it revokes the replicated node.

Advantage:

1. The strategy disperses traffic over the entire network, resulting in small packet loss and considerable energy saving.
2. We show that the proposed solution provides a high detection ratio as well as short detection time for detecting replicas without the use of GPS, as com-pared to existing schemes.
3. The proposed solution is more energy-efficient than existing schemes

IV.CONCLUSION AND FUTURE WORK

In this paper, we proposed a low priced and energy-efficient solved to detect duplicate node for static wireless sensor network. Proposed does not use any additional hardware. Where existingsystem need of expensive hardware like as GPS receiver. Proposed solution use exhibits duplicate node or good performance than existing scheme. When one or more replicas detects within the short duration time and increase the high performance also gain the less energy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

In this paper conclude that the duplicates nodes in Wireless sensor networks are detected by using a new Static testing technique called sequential probability. Using this technique the settlement made with the sensor nodes .nodes is detected efficiently in mobile sensor networks.

REFERENCES

[1]C.P. Mayer, “Security and Privacy Challenges in the Internet of Things,” Electronic Comm. EASST, vol. 17, pp. 1-12, 2009.

[2] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Survey Internet of Things: Vision, Applications and Research Challenges,” J. Ad Hoc Networks, vol. 10, no. 7, pp. 1497-1516, Sept. 2012.

[3] B. Parno, A. Perrig, and V. Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks,” Proc. IEEE Symp. Security and Privacy, pp. 49-63, 2005.

[4] M. Conti, R.D. Pietro, L. Mancini, and A. Mei, “Distributed Detection of Clone Attacks in Wireless Sensor Networks,” IEEE Trans. Dependable and Secure Computing, vol. 8, no. 5, pp. 685-698, Sept. 2011.

[5] C.A. Melchor, B. Ait-Salem, and P. Gaborit, “Active Detection of Node Replication Attacks,” Int’l J. Computer Science and Network Security, vol. 9, no. 2, pp. 13-21, 2009.

[6] H. Choi, S. Zhu, and T.F.L. Porta, “Set: Detecting Node Clones in Sensor Networks,” Proc. Third Int’l Conf. Security and Privacy in Comm. Networks and the Workshops (SecureComm ’07), pp. 341-350, 2007.

[7] Z. Li and G. Gong, “DHT-Based Detection of Node Clone in Wireless Sensor Networks,” Proc. First Int’l Conf. Adhoc Networks, pp. 240-255, 2009.

[8] K. Xing, F. Liu, X. Cheng, and D.H.C. Du, “Real-Time Detection of Clone Attacks in Wireless Sensor Networks,” Proc. 28th Int’l Conf. Distributed Computing Systems (ICDCS ’07), pp. 3-10, 2008.

[9] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, “Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks,” IEEE J. Selected Areas Comm., vol. 28, no. 5, pp. 677-691, June 2010.

[10] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, “Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks,” IEEE Trans. Mobile Computing, vol. 9, no. 7, pp. 913-926, July 2010.

[11] J.-W. Ho, D. Liu, M. Wright, and S.K. Das, “Distributed Detection of Replica Node Attacks with Group Deployment Knowledge in Wireless Sensor Networks,” J. Ad Hoc Networks, vol. 7, no. 8, pp. 1476-1488, Nov. 2009.

[12] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, “Mobile Sensor Network Resilient against Node Replication Attacks,” Proc. Fifth Ann. IEEE Comm. Society Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON ’08), pp. 597-599, June 2008.

[13] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, “Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks,” Proc. IEEE 70th Vehicular Technology Conf. Fall (VTC 2009-Fall), pp. 1-5, Sept. 2009.

[14] J.-W. Ho, M. Wright, and S. Das, “Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis,” Proc. IEEE INFOCOM, pp. 1773-1781, Apr. 2009.

[15] K. Cho, M. Jo, and D.H. Lee, “Effective Distributed Detection of Clones in Mobile Wireless Sensor Networks,” Proc. Int’l Conf. Internet (ICONI), pp. 299-304, Dec. 2009.

[16] K. Xing and X. Cheng, “From Time Domain to Space Domain: Detecting Replica Attacks in Mobile Ad Hoc Networks,” Proc. INFOCOM, pp. 1595-1603, 2010.

[17] J.-W. Ho, M. Wright, and S.K. Das, “Distributed Detection of Mobile Malicious Node Attacks in Wireless Sensor Networks,” J. Ad Hoc Networks, vol. 10, no. 3, pp. 512-523, May 2012.

[18] K. Cho, M. Jo, T. Kwon, H.-H. Chen, and D.H. Lee, “Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks,” IEEE Systems J., vol. 7, no. 1, pp. 26- 35, Mar. 2013.

[19] J.-W. Ho, M. Wright, and S.K. Das, “Zonetrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing,” IEEE Trans. Dependable and Secure Computing, vol. 9, no. 4, pp. 494-510, July- Aug. 2012.