MODELING AND DETECTION OF DISTRIBUTED CLONE ATTACKS FOR SAFETY TRANSACTIONS IN WSN

Suresh.H,
Research Scholar,
Department of Computer Science,
Rayalaseema University,
Kurnool, Andhra Pradesh

Ravindra.S.Hegadi
Associate Professor & Head,
Department of Computer Applications,
Sholapur University,
Sholapur, Maharashtra

Abstract: Wireless Sensor Networks (WSNs) are the type of networks there will be no physical connectivity and are commonly used in often deployed in adverse environments where the attacker can physically capture some of the nodes, first can reprogram, and then, can duplicate them in a large number of clones, easily taking control over the network. Many classical and basic steps are undergone to prevent and eradicate such attacks. But those existing methods are not up to the mark. Basically, WSN are depended on energy aware networks. 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. Our Implementation specifies, user will specify its ID, Location ID, Random number, Destination ID along with Destination Location ID, to the Witness node. The witness will verify the internally bounded user ID with the user specified ID. If the Verification is Success, the packets are sent to the destination. We Propose Modified RED Scheme to identify Cloning attacks in the Network.

Keywords: WSN, Security, Clone Attacks, RED.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate to achieve a common goal [1]. WSNs can be deployed in harsh environments to fulfill both military and civil applications. Due to their operating nature, they are often unattended, hence prone to different kinds of novel attacks. For instance, an adversary could eavesdrop all network communications; further, an adversary could capture nodes acquiring all the information stored therein—sensors are commonly assumed to be not tamper-proof. Therefore, an adversary may replicate captured sensors and deploy them in the network to launch a variety of malicious activities. This attack is referred to as the clone attack since a clone has legitimate information (code and cryptographic material), it may participate in the network operations in the same way as a non compromised node hence, and cloned nodes can launch a variety of attacks [2] [3] [4].

A few have been described in the literature. For instance, a clone could create a black hole, initiate a wormhole attack with a collaborating adversary, or inject false data or aggregate data in such a way to bias the final result. Further, clones can leak data. The threat of a clone attack can be characterized by two main points: A clone is considered totally honest by its neighbors. In fact, without global countermeasures, honest nodes cannot be aware of the fact that they have a clone among their neighbors [5] [6] [7]. To have a large amount of compromised nodes, the adversary does not need to compromise a high number of nodes. Indeed, once a single node has been captured and compromised, the main cost of the attack has been sustained. Making further clones of the same node can be considered cheap. While centralized protocols have a single point of failure and high communication cost, local protocols do not detect replicated nodes that are distributed in different areas of the network. In this work, we look for a network self-healing mechanism, where nodes autonomously identify the presence of clones and exclude them from any further network activity. In particular, this mechanism is designed to iterate as a "routine" event: It is designed for continuous iteration without significantly affecting the network performances, while achieving high clone detection rate [8] [9]. In this paper, we analyze the desirable properties of distributed mechanisms for detection of node replication attack. We also analyze the first protocol for distributed detection, proposed in, and show that this protocol is not completely satisfactory with respect to the above properties. Lastly, inspired by [45], we propose a new randomized, efficient, and distributed (RED) protocol for the detection of node replication attacks, and we prove that our protocol does meet all the above cited requirements. We further provide analytical results when RED and its competitor face an adversary that selectively drops messages that could lead to clone detection. Finally, extensive simulations of RED show that it is highly efficient as for communications, memory, and computations required and shows improved attack detection probability (even when the adversary is allowed to selectively drop messages) when compared to other distributed protocols [10] [11] [12].

II.RELATED WORK

Centralized clone detection protocol in every Network is the existing System. This solution assumes that a random key

pre distribution security scheme is implemented in the sensor network. That is, each node is assigned a set of k symmetric keys, randomly selected from a larger pool of keys . For the detection, each node constructs a counting Bloom filter from the keys it uses for communication. Then, each node sends its own filter to the BS of every network. From all the reports, the BS counts the number of times each key is used in the network. The keys used too often (above a threshold) are considered cloned and a corresponding revocation procedure is raised. Other solutions rely on local detection. A voting mechanism is used within a neighborhood to agree on the legitimacy of a given node. However, this kind of a method applied to the problem of replica detection fails to detect clones that are not within the same neighborhood [13] [14] [15].LSM is used, has only one Witness Node (WN) which Verifies & Detects Cloned Node. Only if the Cloned Node & Original Node sends Packet using the same WN at the same Time, then LSM would detect the Cloned Copy [7] [8].

III.RANDOMIZED, EFFICIENT, AND DISTRIBUTED (RED) PROTOCOL

We propose RED, a new protocol for the detection of clone attacks. RED is similar, in principle, to the Randomized Multicast protocol, but with witnesses chosen pseudo randomly based on a network-wide seed. In exchange for the assumption that we are able to efficiently distribute the seed, RED achieves a large improvement over RM in terms of communication and computation.

Nodes are registered in a Location. Group Leader is elected, then the Group Leader will start transmit a Ransom Number to all the nodes which are attached to that Group Leader (GL). If a node A in the Location 1 wants to send a data to another node D in the Location 4, then the following steps are carried.

- Node ID of A + Location ID of A – 1 + Random Number of GL (1) + Time Stamp + Destination ID of Node D + Location ID of D – 4 ---------- (1)
- Internal Sender Node ID and Location ID is also appended with 1.
- Encrypt 1 with RSA Algorithm then send to the Witness Node.
- Witness node will Decrypt 1, then will compare with User Specified Node ID and Location ID with internally appended Node ID and Location ID, which is original.
- If the both those user specified and internally appended information's are matched, then the witness node will check the Random number with respect to the Time Stamp by sending the request to the Group Leader of the Location 1.
- The Group Leader will transmit Random Number which was generated with respect to that Time Stamp to the Witness node.
- Witness node will check the Random number which is generated with the User information. If both the data are matched then the Witness node will confirm that this node is Genuine.
- Only if the Witness node confirms the Sender node, the data is send to the Destination, which is Genuine.
- If user specified information and the internal information are varied then the Witness node will identify that Cloning or some Mal practice has occurred and the Packets are discarded by the witness node.

RED is used in which Group Leader (GL) is elected. GL will multicast a Random Number (RN) to all its Group Nodes at a Time Stamp (TS). RED will Verify RN, Node ID, Location ID,TS via WN which is Encrypted automatically from the User and Decrypted and Verified by the WN. Here we maintain Multiple WN.The modification is which we propose is to compare the RN & also the Node ID given by the user and the Original Node ID appended with the data. The complete scenario has been depicted in the Figure 1.

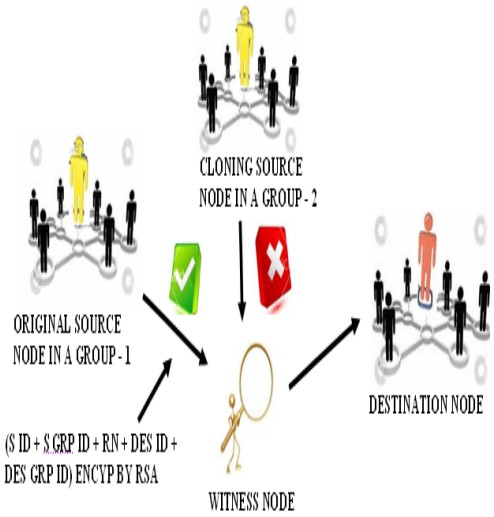

Figure 1: RED Protocol

IV.CONCLUSION

In Wireless sensor network there were many attacks which tamper the proper communication. Among such various attacks Cloning attack is one of the major attacks. In this paper we detected such cloning attack by our proposed novel methodology called RED protocol. BY this protocol we can have secure authenticated transactions can happen in the wireless sensor networks. In future, we are intended to provide higher security with large complex and real networks using different network quality of service parameters.

V.REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Int'l J. Computer and Telecomm. Networking, vol. 38, no. 4, pp. 393-422, 2002.

[2] R. Anderson and M.G. Kuhn, "Tamper Resistance—A Cautionary Note," Proc. USENIX '96 Workshop, pp. 1-11, 1996.

[3] A. Becher, Z. Benenson, and M. Dornseif, "Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks," Proc.Int'l Conf. Security in Pervasive Computing (SPC '06), pp. 104-118,2006.

[4] C. Bettstetter, "On the Minimum Node Degree and Connectivity of a Wireless Multihop Network," Proc. MobiHoc '02, pp. 80-91, 2002.

[5] C. Bettstetter and C. Hartmann, "Connectivity of Wireless Multihop Networks in a Shadow Fading Environment," Proc. Int'l Workshop Modeling Analysis and Simulation of Wireless and Mobile Systems (MSWiM '03), pp. 28-32, 2003.

[6] R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T.Kandemir, "On the Detection of Clones in Sensor Networks Using Random Key Predistribution," IEEE Trans. Systems, Man and Cybernetics, Part C: Applications and Rev., vol. 37, no. 6, pp. 1246-1258, Nov. 2007.

[7] KS Praveen, HL Gururaj, B Ramesh "Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols" Elsevier Procedia Computer Science 85, 325-330

[8] A. Caruso, A. Urpi, S. Chessa, and S. De, "Gps-Free Coordinate Assignment and Routing in Wireless Sensor Networks," Proc.IEEE INFOCOM '05, pp. 150-160, 2005.

[9] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. Symp. Security and Privacy (S&P '03), pp. 197-213, 2003.

[10] G. Chen, J.W. Branch, and B.K. Szymanski, "Local Leader Election, Signal Strength Aware Flooding, and Routeless Routing,"Proc. IEEE Int'l Parallel and Distributed Processing Symp.(IPDPS '05), p. 244.1, 2005.

[11] H. Choi, S. Zhu, and T.F. La Porta, "SET: Detecting Node Clones in Sensor Networks," Proc. Int'l Conf. Security and Privacy in Comm. Networks and the Workshops (SecureComm '07), pp. 341-350, 2007.

[12] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," Proc. IMA Int'l Conf. '01, pp. 360-363, 2001.

[13] M. Conti, R. Di Pietro, A. Gabrielli, L.V. Mancini, and A. Mei, "The Quest for Mobility Models to Analyse Security in Mobile Ad Hoc Networks," Proc. Seventh Int'l Conf. Wired/Wireless Internet Comm.
(WWIC '09), pp. 85-96, 2009.

[14] M. Conti, R. Di Pietro, and L.V. Mancini, "Secure Cooperative Channel Establishment in Wireless Sensor Networks," Proc. IEEE Pervasive Computing and Comm. (PERCOM '06) Workshop, pp. 327- 331, 2006.

[15] M. Conti, R. Di Pietro, and L.V. Mancini, "ECCE: Enhanced Cooperative Channel Establishment for Secure Pair-Wise Communication in Wireless Sensor Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 49-62, 2007.

