IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Optimized Replica Node Attack Detection Technique in Wireless Sensor Networks Using Hypothesis Testing

P.R. Libiya Shaljat Rose[*1] , R. Manickavasagam[2]

[*1]P.G Student, M.E CSE, Alpha college of Engg , Chennai, T.N, India.

[2]Professor, Head of the Dept of ECE, Alpha College of Engg , Chennai, T.N, India

libileni@gmail.com

Abstract

In wireless sensor network, there are number of small sensor nodes, this sensor nodes are organized into clusters and send some report to base station. An attacker can capture sensor nodes and can compromise sensor nodes. Then would create duplicate nodes and built up various attacks using duplicate nodes, inserts into the network. This is happened because of unattended nature of wireless sensor network. These attacks helps attacker to control few more nodes to have control over the network. There are many node replication attack detection methods which have been used to secure from attacks in the sensor network where nodes are static. These methods are dependent on fixed location of sensors and hence do not works for sensor network where nodes are mobile. In this method basic idea is used that mobile node never have more speed than system speed. In this work, an optimized replica node attack detection technique in wireless sensor networks by using hypothesis testing.

Keywords: Wireless sensor networks, security, replica attack detection, mobile sensor networks, hypothesis testing.

Introduction

Wireless sensor network is a collection of nodes organized into a cooperative network. These advanced sensor network architectures could be used for a variety of applications including intruder detection, border monitoring, and military patrols. In potentially hostile environments, the security of unattended mobile nodes is extremely critical. The adversary can compromise the captured nodes and obtain all the secrets of the nodes, replicate the compromised nodes to get many replicas with the same node identity. Then adversary can launch an insidious attack with these legitimate nodes [3]. Replica nodes need not be identical robots; a group of static nodes can mimic the movement of a robot and other mobile nodes or even humans with handheld devices could be used. The only requirement is that they have the software and keying material to communicate in the network, all of which can be obtained from the captured node. The adversary can then leverage this insider position in many ways. Alternately, it could jam legitimate signals from benign nodes or inject falsified data to corrupt the sensors' monitoring operation [1]. A more aggressive attacker could undermine common network protocols, including cluster formation, localization, and data aggregation, thereby causing continual disruption to network operations. Through these methods, an adversary with a large number of replica nodes can easily defeat the mission of the deployed network. Thus, it needs to detect and revoke the sources of attacks as soon as possible to substantially reduce the costs and damages incurred by employing attack-resilience approach. The principle sources of various attacks are compromised sensor nodes in the sense that attacker can compromise sensor nodes by exploiting the unattended nature of wireless sensor networks and thus do any malicious activities with them. However, most of them focus on making the protocols be attack resilient rather than removing the source of attacks. Although attack resiliency approach mitigates the threats on the network services and communication protocols, this approach requires substantial time and effort to continuously enhance the robustness of the protocols in accordance with the emergence of new types of attacks [4]. Moreover, since it is hard to predict new types of attacks, the protocols will likely have resiliency only after being damaged by new types of attacks. Accordingly, captured nodes would not participate in any network operations during that period. By leveraging this intuition, it detects captured nodes by using the hypothesis Testing. The main advantage of our scheme is to quickly detect captured nodes by using hypothesis testing. Dangerous attack is the replica node attack, in which the adversary takes the secret keying materials from a compromised node, generates a large number of attacker controlled replicas that share the compromised node's keying

materials and ID, and then spreads these replicas throughout the network. With a single captured node, the adversary can create as many replica nodes as it has the hardware to generate. The time and effort needed to inject these replica nodes into the network should be much less than the effort to capture and compromise the equivalent number of original nodes. The replica nodes are controlled by the adversary, but have keying materials that allow them to seem like authorized participants in the network. Protocols for secure sensor network communication would allow replica nodes to create pair wise shared keys with other nodes and the base station, thereby enabling the nodes to encrypt, decrypt, and authenticate all of their communications as if they were the original captured node. The hypothesis testing is a statistical decision process that comes to a decision with multiple pieces of evidence. It is also considered to be one-dimensional random walk with lower and upper limits. The mobile node's measured speed is over the system-configured maximum speed, it is then highly likely that at least two nodes with the same identity are present in the network. To minimize these false positives and false negatives, by applying the hypothesis test, a hypothesis testing method that can make decisions quickly and accurately. By performing the hypothesis testing on every mobile node, using a null hypothesis that the mobile node has not been replicated and an alternate hypothesis that it has been replicated. By using this testing, the occurrence of a speed that is less than or exceeds the system-configured maximum speed will lead to acceptance of the null or alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network.

Network Assumptions

In this network, mobile sensor devices are more powerful than stationary ones in terms of battery power, storage and communication band. The mobile nodes are also able to obtain their location information. The sensors organize a two-dimension stationary sensor network where the locations of sensors do not change after deployment It assume that all direct communication links between nodes are bidirectional. Every node has a unique ID in the network which is assigned by the network operator before deployment. An identity-based public key scheme and time synchronization system are employed for the nodes and network as the most common attack detection scheme [6, 7]. It also assumes there is a maximum speed of the mobile nodes in this system as Ho et al. [6]. This maximum speed assumption can be used to identify the replicas of mobile nodes if they move faster than the speed limitation. The adversary has the ability to compromise a limited number of nodes, fully control the compromised node, and produce many replicas of compromised nodes to enlarge the attack ability. It assumes that the adversary can't capture enough nodes to have a significant influence on the network, but may fully control the whole network by replicating many replicas. It also assumes that the adversary can't create new IDs [5]. Thus the goal of this paper is finding and revoking all the replicas with the same ID to ensure the security of the network.

Proposed System

A novel mobile replica node attack detection technique based on hypothesis testing. By using the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. A straightforward solution to stop replica node attacks is to prevent the adversary from extracting secret key materials from mobile nodes by equipping them with tamper-resistant hardware. Proposed system is beneficial since it turned into information system analysing hypothesis testing. That will meet the organizations operating requirements. After physically capturing and compromising a few sensor nodes, attacker can generate many replica nodes with the same ID and secret keying materials as the compromised nodes, and mount a variety of attacks with replica nodes. It considers a two-dimensional mobile sensor network where sensor nodes freely roam throughout the network. This assumes that every mobile sensor node's movement is physically limited by the system-configured maximum speed. Also, assume that all direct communication links between sensor nodes are bidirectional. This communication model is common in the current generation of sensor networks. The simulation results of both cases show that this scheme very quickly detects mobile replicas with low false positive and negative rates. It validates the effectiveness, efficiency, and robustness of our scheme through analysis and simulation experiments. The result will be the proposed mobile replica detection scheme using the hypothesis testing along with security and performance analyses.

Attacker Detection Technique

Regarding errors in the measurement of time and location, it can consider both random and systematic errors. Since speed is measured based on location and time, the errors can come from either measurement. The time of each claim is measured and verified by the requesting node, rather than the measured node. Since claim verification and forwarding is done probabilistically, the chance of having two verified and forwarded claims from the

same requesting node is low. Thus, systematic time measurement error at the requesting node is likely to result in independent errors between each location claim for the nodes being measured. Systematic location measurement error means that the measurements are not independent. However, assume that the measurement error is consistent and biased in one direction, and then the speed of a node will be measured accurately in most cases. Random location measurement errors are more likely to lead to errors in speed measurement. A malicious node u may attempt to forge a claim, either by sending a claim with incorrect data or by sending a claim with a bad signature.

Replica Node Detection Using Hypothesis Testing

The hypothesis testing can be thought of as one-dimensional random walk with the lower and upper limits. Before the random walk starts, null and alternate hypotheses are defined in such a way that the null hypothesis is associated with the lower limit while the alternate one is associated with the upper limit. A random walk starts from a point between two limits and moves toward the lower or upper limit in accordance with each observation. The base station computes the speed from every two consecutive claims of a mobile node and performs the hypothesis testing by considering speed.

Experimental Setup

Using ns2 simulator the nodes are created. Initially the nodes are deployed in the network after deploying the nodes the base station sends the coverage region to all the nodes. Then the sensor nodes gather the data and sent to the base station, the base station verifies the data. If the data gets dropped then the nodes won't send the data to the base station otherwise the replicated nodes send the false data to the base station. The functionality replica nodes disrupt the network operations. Using sensor speed can detect the replica node. If the sensor node speed is within than the system configuration speed than that node is take as a uncompromised node. If the node speed is greater than the system configuration speed that node is taken as a compromised node and if any of this node is death in the particular location the neighbour node will take care of that particular region and sense the data and finally secure communication takes place.

Simulation Results

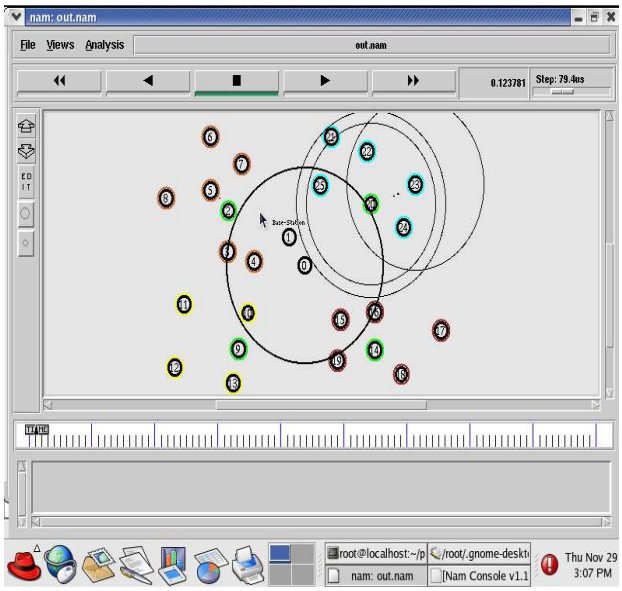

Figure: 1 design of mobile sensor networks

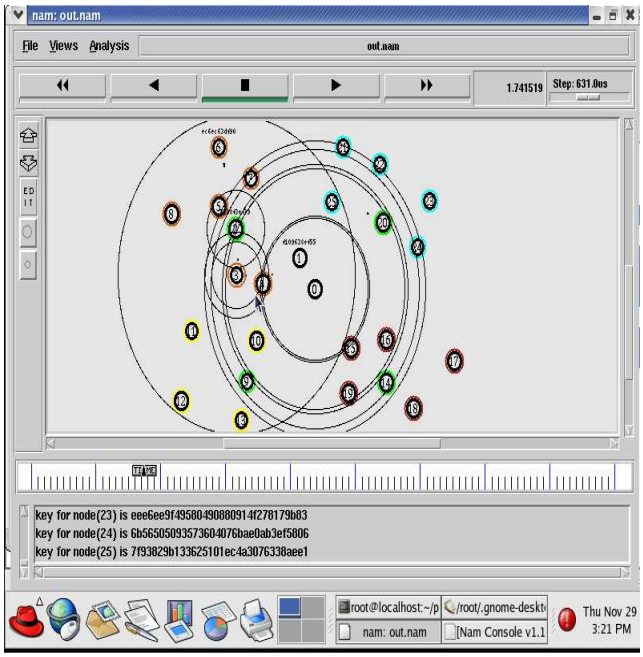

Figure: 2 sending and receiving data

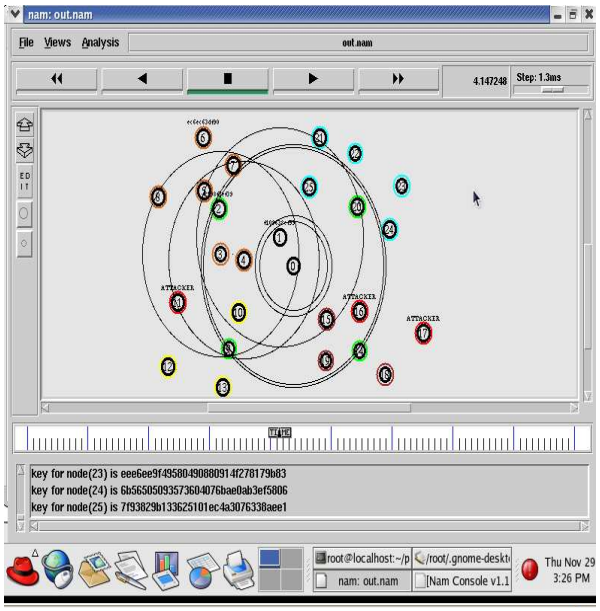

Figure: 3 detection of replica node

Conclusion

This paper concludes that replica node attack in wireless senor networks are detected by using technique called hypothesis testing. Proposed a node capture attack detection scheme using the hypothesis Testing. By performing the hypothesis testing on every mobile node using a null hypothesis that the mobile node has not been replicated and an alternate hypothesis that it has been replicated. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network. It has analytically demonstrated the limitations of attacker strategies to evade our detection technique. It validates the effectiveness, efficiency, and robustness of our scheme through analysis and simulation experiments. The results of these simulations show that our scheme quickly detects mobile replicas with a small number of location claims against either strategy.

References

[1] Capkun, S. & Hubaux, J.P. (2006). Secure positioning in wireless networks. IEEE Journal on Selected Areas in Communications, 24(2):221-232, February 2006

[2] Chan, H., Perrig, A., & Song, D. (2006). Secure hierarchical in-network aggregation in sensor networks. In ACM CCS, pages: 278-287, October 2006.

[3] Conti, M., Pietro, R., Mancini, L., & Mei, A. (2008). Emergent Properties: Detection of the Node-capture Attack in Mobile Wireless Sensor Networks. In ACM WiSec, April 2008

[4] H. Choi, S. Zhu, and T.F La Porta. SET: Detecting node clones in Sensor Networks. In IEEE/CreateNet Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm), 2007.

[5] S. ˇCapkun and J.P. Hubaux. Secure Positioning in Wireless Networks. IEEE Journal on Selected Areas in Communications, 24(2):221–232, February 2006

[6] Parno B, Perrig A, Gligor VD. Distributed detection of node replication attacks in sensor networks.Proceedings of IEEE S&P; Oakland, CA, USA. 8–11 May 2005; pp. 49–63.

[7] Ho JW, Wright M, Das SK. Fast detection of replica node attacks in mobile sensor networks using sequential analysis. Proceedings of IEEE INFOCOM; Rio de Janeiro, Brazil. 19–25 April 2009; pp. 1773–1781.