Middle-East Journal of Scientific Research 20 (4): 522-526, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.20.04.12034

Quick Detection Involving Cellular Duplicate Node Assaults in Cellular Sensor Networks Using SPRT

A. Rama and M. Masthan

Bharath University,
Tagore Engineering College, India

Abstract: The wireless sensor networks, an adversary can capture and compromise sensor nodes, make replicas of them and then mount a variety of attacks with these replicas. These replica node attacks are dangerous because they allow the attacker to leverage the compromise of a few nodes to exert control over much of the network. Several replica node detection schemes have been proposed in the literature to defend against such attacks in static sensor networks. However, these schemes rely on fixed sensor locations and hence do not work in mobile sensor networks, where sensors are expected to move. In this work, we propose a fast and effective mobile replica node detection scheme using the Sequential Probability Ratio Test. To the best of our knowledge, this is the first work to tackle the problem of replica node attacks in mobile sensor networks. We show analytically and through simulation experiments that our scheme detects mobile replicas in an efficient and robust manner at the cost of reasonable overheads. Index Terms-Replica detection, sequential analysis, mobile sensor networks, security.

Key words: Replica node attacks · Static sensor · Replica node detection · Experiments

INTRODUCTION

The time and effort needed to inject these replica nodes with sensing, wireless communications and movement into the network should be much less than the effort to capabilities, are useful for tasks such as static sensor capture and compromise the equivalent number of original deployment, adaptive sampling, network repair and event nodes. The replica nodes are controlled by the adversary, detection [1-7] . These advanced sensor network architectures but have keying materials that allow them to seem like could be used for a variety of applications including authorized participants in the network. Protocols for secure intruder detection, border monitoring and military patrols. sensor network communication would allow replica nodes In potentially hostile environments, the security of un-to create pair wise shared keys with other nodes and the attended mobile nodes is extremely critical. The attacker base station, thereby enabling the nodes to encrypt, decrypt, may be able to capture and compromise mobile nodes and authenticate all of their communications as if they were then use them to inject fake data, disrupt network the original captured node. operations and eavesdrop on network communications. The adversary can then leverage this insider position in.

Dangerous attack is the many ways. For example, the monitor agent can simply monitor a replica node attack, in which the adversary takes the significant fraction of the network traffic that would pass secret keying materials from a compromised node, gen-through these nodes. Alternately, we could jam legitimate a large number of attacker-controlled replicas that signals from benign nodes or inject falsified data to corrupt share the compromised node's keying materials and ID and the sensors' monitoring operation. A more aggressive then spreads these replicas throughout the network. With a attacker could undermine common network protocols, single captured node, the adversary can create as many including cluster formation, localization and data aggregareplica nodes as he has the hardware to generate. Note that tion, thereby causing continual disruption to network replica nodes need not be identical robots; a group of static operations. Through these methods, an adversary with a nodes can mimic the movement of a robot and other mobile large number of replica nodes

Corrseponding Author: A. Rama, Bharath University, Tagore Engineering College, India.

can easily defeat the mission nodes or even humans with handheld devices could be of the deployed network.

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 [8-9]. We might expect such measures to be implemented in mobile nodes with security-critical missions. However, although tamper resistant hardware can make it significantly harder and more time-consuming to extract keying materials from captured nodes, it may still be possible to bypass tamper resistance for a small number of nodes given enough time and attacker expertise. Adversary can generate many replicas from a single captured node, this means that replica attacks are even more dangerous when compared with the possibility of compromising many nodes. We thus believe that it is very important to develop software-based countermeasures to defend mobile sensor networks against replica node attacks. Several software-based replica node detection schemes have been proposed for static sensor networks. 54 The primary method used by these schemes is to haven odes report location claims that identify their positions and for other nodes to attempt to detect conflicting reports that signal one node in multiple locations. However, since this approach requires fixed node locations, it cannot be used when nodes are expected to move. Thus, our challenge is to design an effective, fast and robust replica detection scheme specifically for mobile sensor networks. In this paper, we propose a novel mobile replica detection scheme based on the Sequential Probability Ratio Test (SPRT) [10-13]. We use the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. As a result, a benign mobile sensor node's measured speed will nearly always be less than the system-configured maximum speed as long as we employ a speed measurement system with a low error rate. On the other hand, replica nodes are in two or more places at the same time. This makes it appear as if the replicated node is moving much faster than any of the benign nodes and thus the replica nodes' measured speeds will often be over the system-configured maximum speed.Accordingly, if we observe that a mobile node's measured speed is over the systemconfigured maximum speed, it is then highly likely that at least two nodes with the same identity are present in the network. However, if the system decides that a node has been Replicated based on a single observation of a node moving faster than it should, we might get many false positives because of errors in speed measurement. Raising the speed hreshold or other simple ways of compensating can lead to high false negative rates. To minimize these false positive sand false negatives, we apply the SPRT, a hypothesis testing method that can make decisions quickly and accurately. We perform the SPRT 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. In using the SPRT, 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. We validate the effectiveness, efficiency and robustness of our scheme through analysis and simulation experiments. Specifically, we find that the min attack against the SPRT based scheme is when replica nodes fail to provide signed location and time information for speed measurement. To overcome this attack, we employ a quarantine defense technique to block the noncompliant nodes. We study this technique in two ways. First, we show through quarantine analysis that the amount of time, during a given time slot, that the replicas can impact the network is very limited.

Related Work: The first work on detecting replica node attacks is due to who proposed randomized and lineselected multicast schemes to detect replicas in static wireless sensor networks. In those two schemes, nodes report location claims that identify their positions and attempt to detect conflicting reports that signal one node in multiple locations.. proposed a scheme to enhance the lineselected multicast scheme of in terms of replica detection probability, as well as storage and computation overheads by using trusted random values.proposed several schemes for distributed detection of replica nodes that take advantage of group deployment knowledge to reduce the communication, computation and storage overheads required for replica detection and improve on the replica detection capability of the line-selected scheme. proposed a fingerprint-based replica node detection scheme. In this scheme, nodes report fingerprints, which identify a set of their neighbors, to the base station. The base station performs replica detection by using the property that fingerprints of replicas conflict each other. However, none of these solutions is suitable for replicanode detection in mobile sensor networks. If the scheme are used in mobile sensor networks, sensor

nodes' location claims will be continuously changed in accordance with their movements and thus location claims from the same benign node will always conflict each other. Similarly, if the scheme is used in mobile sensor networks, mobility will continuously make nodes have different fingerprints and thus fingerprints of the same benign node will conflict each other. The proposed schemes to detect node replica attacks in mobile sensor networks. The key idea is to detect mobile replicas by leveraging the intuition that the number of mobile nodes encountered by mobile replicas in a time interval is more than the number encountered by a benign mobile node. It detects mobile replicas in fully distributed manner, while our scheme relies on the base station for mobile replica detection. However, replicas can this detection technique by carefully controlling the number of encounters each replica has with other nodes. The attacker can selectively uses its encounters to maximize the effectiveness of the attacks it is trying to mount with the replicanodes. Since this puts a limitation on the attacker, it remains to be studied whether the detection scheme is enough to deter effective replica attacks.

The Proposed Approach: The proposed system enabling node to encrypt and decrypt.Mobile replica detection is based on Sequencial Hypothesis Testing.

Network Assumptions: It is a two-dimensional mobile sensor network where sensor nodes freely roam throughout the network. It assume that every mobile sensor node's movement is physically limited by the system-configured maximum speed, Vmax. It also assume that all direct communication links between sensor nodes are bidirectional. This communication model is common in the current generation of sensor networks. It assume that every mobile sensor node. Is capable of obtaining its location information and also verifying the locations of its neighboring nodes. This can be implemented by employing secure localization methods. 55 It assume that the clocks of all nodes are loosely synchronized. This can be achieved with the help of secure time synchronization protocols .It also assume that the nodes in the mobile sensor network communicate with a base station.The base station may be static or mobile, although we focus on a static base station for our simulations, as long as the nodes have a way to communicate reliably to the base station on a regular basis.

Attacker Models: It assume that an adversary may compromise and fully control a subset of the sensor nodes, enabling amount various kinds of attacks. Attacker can inject false data packets into the network and disrupt local control protocols such as localization, time synchronization,and route discovery process.the place some limits on the ability of the adversary to compromise nodes. We note that if the adversary can compromise a major fraction nodes of the network, he will not need nor benefit much from the deployment of replicas.To amplify his effectiveness, the adversary can also launch a replica node attack, which is the subject of our investigation. It assume that the adversary can produce many replica nodes and that they will be accepted as a legitimate part of the network. It also assume that the attacker attempts to employ as many replicas of one or more compromised sensor nodes in the network as will be effective for his attacks. The attacker can allow his replica nodes to randomly move or he could move his replica nodes in different patterns in an attempt to frustrate our proposed scheme. It assume that the base station is a trusted entity.This is a reasonable assumption in mobile sensor networks,because the network operator collects all sensor data and can typically control the nodes' operation through the base station. Thus, the basic mission of the sensor network is already completely undermined if the base station is compromised.

Mobile Replicadetectionusingsprt: These technique to detect replica node attacks in mobile sensor networks.In static sensor networks, a sensor node is regarded as being replicated if it is placed in more than one location. If nodes are moving around in network, however, this technique does not work, because a benign mobile node would be treated as a replica due to its continuous change in location. Hence, we must use some other technique to detect replica nodes in mobile sensor networks. Fortunately, mobility provides us with a clue to help resolve the mobilereplica detection problem. Specifically, a benign mobile sensor node should never move faster than the systemconfigured maximum speed, Vmax. As a result, a benign mobile sensor node's measured speed will appear to be at most Vmax as long as we employ a speed measurement system with a low rate of error. On the other hand, replica nodes will appear to move much faster than benign nodes and thus their measured speeds will likely be over Vmax because they need to be at two (or more) different places at once. Accordingly, if the mobile node's measured speed exceeds Vmax, it is then highly likely that at least two nodes with the same identity are present in the network. The project propose a mobile replica detection scheme by leveraging this intuition. Our scheme is based on the Sequential Probability Ratio Test which is a statistical

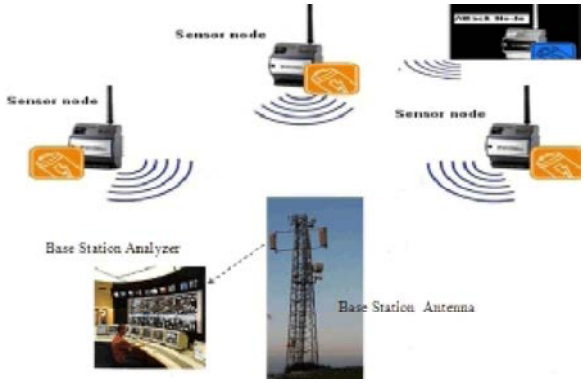

Fig. 1: SystemArchitecture

decision process.The SPRT can be thought of as onedimensional 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. If the walk reaches (or exceeds) the lower or upper limit, it terminates and the null or alternate hypothesis is selected, respectively. The SPRT is well suited for tackling the mobile replica detection problem since we can construct a random walk with two limits in such a way that each walk is determined by the observed speed of a mobile node. The lower and upper limits can be configured to be associated with speeds less than and in excess of Vmax, respectively.the SPRT to the mobile replica detection problem as follows: Each time a mobile sensor node moves to a new location, each of its neighbors asks for a signed claim containing its location and time information and decides probabilistically whether to forward the received claim to the base station.

Limitations of Replica Node Attacks: Let us now discuss ways in which the attacker could attempt to evade our detection scheme and defensive counter measures that we can employ.First, a malicious node u may attempt to forget a claim,either by sending a claim with incorrect data or by sending a claim with a bad signature. However, all of u's neighbours will check the validity of u's identity, reported location, reported time and the signature over these values using node u's public key. Alternatively, node u can simply ignore the 56 claim requests. In our scheme, if u's benign neighbor does not receive a claim despite sending a claim request, it will remove u from its neighboring set and will not communicate with u. It note that if one of u's neighbors is malicious, the malicious node can serve as u's neighbor for forwarding packets. However, there is little benefit to the attacker of having a replica node in the same area as another compromised node. The compromised node can just as easily report fake data, participate in local control protocols,and eavesdrop on messages sent through it. Furthermore, if the attacker needs one compromised node to accompany each replica node in the network, there will be a very high cost for replica node attacks.Similarly, an attacker will not gain much benefit from having multiple replicas of a single node form a group that always moves together and stays close enough so that all replicas can claim the same location. This is because these nodes would essentially have the same set of neighbors. Consider a compromised node u and its replica u communicating with neighboring node v. From v's perspective, there is no difference between the two replicas and v treats all messages as coming from a single node. The two nodes thus cannot do anything that a single compromised node u could not do by itself. If the replicas can claim the same location while reaching a slightly larger set of neighbors, then the attacker can gain a small amount of additional influence through the replica attack, but no more than it could gain with a better antenna and more signal power. An interesting variant of this attack, however, is to keep replicas close to each other so that the perceived velocity between their location claims is less than Vmax. To do this, an attacker coordinates a set of replicas to respond with correct claims only to those claim requests that make it appear as a single node never moving faster than Vmax.

CONCLUSION

The project proposed a replica detection scheme for mobile sensor networks based on the SPRT. It has analytically demonstrated the limitations of attacker strategies to evade our detection technique. In particular, we first showed the limitations of a group attack strategy in which the attacker controls the movements of a group of replicas.It presented quantitative analysis of the limit on the amount of time for which a group of replicas can avoiddetection and quarantine. It also modeled the interaction between the detector and the adversary as a repeated game and found a Nash equilibrium. This Nash equilibrium shows that even the attacker's optimal gains are still greatly limited by the combination of detection and quarantine. It performed simulations of the scheme under a random movement attack strategy in which the attacker lets replicas randomly move in the network and under a static placement attack strategy in which he

keeps his replicas from moving to best evade detection. 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. Matthew Wright, 2011. Fast Detection of Mobile ReplicaNode Attacks in WSN Using SPRT" IEEE Transaction on Mobile Computing, 10(6).
2. Ho, D., Liu, M. Wright and S.K. Das, 2009. Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks," Ad Hoc Networks, 7(8): 1476-1488.
3. Ho, J., M. Wright and S.K. Das, Apr. 2009. Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis," Proc. IEEE INFOCOM, pp:1773-1781.
4. Conti, M., R.D. Pietro, L.V. Mancini and A.Mei, 2007. "A Randomized, Efficient and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks," Proc. ACM Mobi Hoc, pp: 80-89.
5. Capkun, S. and J.P. Hubaux, 2006. Secure Positioningin Wireless Networks," IEEE J. Selected Areas in Comm, 24(2): 221232.
6. Boudec, J.Y.L. and M. Vojnovicc, 2005. "Perfect Simulation and Stationary of a Class of Mobility Models," Proc. IEEE INFOCOM, pp: 2743-2754.
7. Dantu, K., M. Rahimi, H. Shah, S. Babel, 2005. A Dhariwal and G.S. Sukhatme, "Robomote: Enabling Mobility in Sensor Networks," Proc. Fourth IEEE Int' Symp. Information Processing in Sensor Networks (IPSN), pp: 404-409.
8. Hu, L. and D. Evans, 2004. "Localization for Mobile Sensor Networks," Proc. ACM Mobi Com, pp: 45-57.
9. Abou-Deif, M.H., M.A. Rashed, M.A.A.Sallam, E.A.H. Mostafa and W.A. Ramadan, 2013, Characterization of Twenty Wheat Varieties by ISSR Markers, Middle-East Journal of Scientific Research, 15(2): 168-175.
10. Kabiru Jinjiri Ringim, 2013. Understanding of Account Holder in Conventional Bank Toward Islamic Banking Products, Middle-East Journal of Scientific Research, 15(2): 176-183.
11. Muhammad Azam, Sallahuddin Hassan and Khairuzzaman, 2013. Corruption, Workers Remittances, Fdi and Economic Growth in Five South and South East Asian Countries: A Panel Data Approach Middle-East Journal of Scientific Research, 15(2): 184-190.
12. Sibghatullah Nasir, 2013. Microfinance in India: Contemporary Issues and Challenges, Middle-East Journal of Scientific Research, 15(2): 191-199.
13. Mueen Uddin, Asadullah Shah, Raed Alsaqour and Jamshed Memon, 2013. Measuring Efficiency of Tier Level Data Centers to Implement Green Energy Efficient Data Centers, Middle-East Journal of Scientific Research, 15(2): 200-207.