Detection of Mobile Replica Node Attacks in Mobile Computing Environment Using GUIDE Technique

M.SUBATHIRA DEVI,
MTECH – CSE,
PRIST UNIVERSITY,
PUDHUCHERRY.
devi.vinosuba87@gmail.com

MRS. BHARATHI,
ASST.PROFESSOR,
DEPARTMENT OF CSE,
PRIST UNIVERSITY,
PUDHUCHERRY,
prist2009cse@gmail.com

ABSTRACT

Mobile computing is a term used to refer to a variety of devices that allow accessing data and information from anytime, anyplace, anywhere. The mobile networks are often deployed in complex environments in which to provide a secure transmission and also to detect the hackers. An adversary can capture and compromise mobile nodes, generate replicas of those nodes, and mount a variety of attacks with the replicas injects into the network. These attacks are dangerous because they allow the attacker to leverage and compromise of a few nodes to exert control over much of the network. Thus adversaries can capture some nodes, replicate them and deploy those replicas back into the strategic positions in the network to launch a variety of attacks. These are referred to as node replication attacks. Some methods of defending against node replication attacks have been proposed only in static networks. This paper proposes the work for mobilenetworks for detecting replica node attack. In this scenario, one of the dangerous attacks is the *replica 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 node's keying materials and ID, and then spreads these replicas throughout the network. To prevent and avoid such replica nodes, each and every node has its own spread value generated by pseudo random number which is registered in base station including IP address along with their secret keying materials.Whenever mobile node sends packet through base station by transmission channel, at the time detection and verification of nodes were performed by applying GUIDE technique. Then the base station allows broadcasting the packets and reaching destination IP address. Thereby we can avoid the replica node attacks and also provide information of intruders in efficient manner to achieve effective and robust replica detection capability with reasonable overheads.

Index Terms- Replica node reduction, Mobile Node, Pseudo random number, GUIDE technique

1. INTRODUCTION

Mobile computing is a generic term used to refer to a variety of devices that allow people to access data and information from everywhere. The definition of "replica" has emerged that defines one as a copy of an original object. Replica is the process of compromising the original mobile node. There are many issues in mobile computing like insufficient bandwidth, security standards, power consumption, Transmission Interferences and Potential health hazards. As oppose to the benefits of being able to access information from any location through wireless transmission, there is it

faults with the need for security protection. In a wireless mobile communication environment, the messages transmitted over the wireless medium are more susceptible to eavesdropping than in a wired network. Also, it is possible for any user to access the mobile communication system using false identity. Advances in robotics have mad e it possible to develop a variety of new architectures for autonomous wireless networks. Mobile computing network architectures could be used for a variety of applications including intruder detection, border monitoring, and military patrols in a wireless network. In potentially hostile environments, the security of unattended mobile nodes is extremely critical. The attacker may be able to capture and compromise mobile nodes, and then use them to inject fake data, disrupt network operations, and eavesdrop on network communications. In this scenario, a particularly 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 [1].By the extraction of key material from the benign node, the attacker can create replica node and allow them to seem like authorized participants in the network. The adversary can then leverage this insider position in many ways. For example, he can simply monitor a significant fraction of the network traffic that would pass through these nodes. Alternately, he could jam legitimate signals from benign nodes or inject falsified data to corrupt the monitoring operation.

2. RELATED WORK

Several software-based replica node detection schemes have been proposed for static networks [5], [9], [13]. The primary method used by these schemes is to have location report of the nodes and identify their positions. The drawback of this approach may cause of generating the conflict reports whose signal of one node from multiple locations. However, 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 networks. In the randomized multicast scheme, every node is required to multicast a signed *location claim* [12] to randomly chosen witness nodes. A witness node that receives two conflicting location claims for a node concludes that the node has been replicated and initiates a process to revoke the node. The line-selected multicast scheme, on the other hand, reduces communication overhead of the randomized multicast scheme by having every claim-relaying node participate in the replica detection and revocation process.

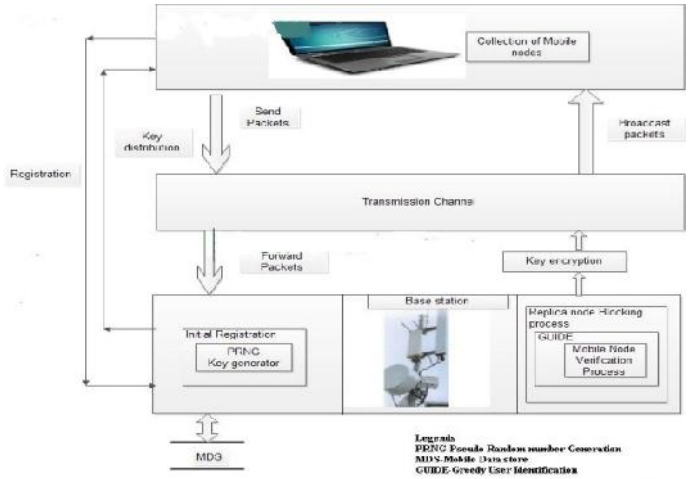
3. SIGNIFICANCE OF WORK

We propose this paper to overcome the drawback from replica node attack in mobile computing environment. Mobile computing has many advantages like improved decision making, increased productivity and reduced costs. By taking advantage, the proposed schemes perform replica detection in a distributed, efficient, and secure manner. Through analysis experiments that our scheme will achieve effective and robust replica detection capability with substantially lower communication, computational, and storage overheads than prior work in the literature. 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 network communication would allow replica nodes to create pair wise shared keys with other nodes and the base station, thus enabling the nodes to encrypt and authenticate all of their communications as if they were the original captured node.

4. PROPOSED WORK

In this work, we seek ways to achieve effective and robust replica node detection capability with lower communication, computation, and storage overheads than prior work. We assume that an adversary may compromise and fully control a subset of the mobile nodes, enabling him to mount various kinds of attacks. For instance, he can inject false data packets into the network and disrupt local control protocols. Furthermore, he can launch denial-of-service attacks by jamming the signals from benign nodes. However, we 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 [1].To amplify his effectiveness, the adversary can also launch a replica node attack, which is the subject of our investigation. We assume that the adversary can produce many replica nodes and that they will be accepted as a legitimate part of the network. We also assume that the attacker attempts to employ as many replicas of one or more compromised 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.We propose an algorithm called GUIDE for the identification of compromised users in the system based onthe set of control channels that are jammed. We evaluate the estimation error using the GUIDE [17] algorithm in terms of the false alarm and miss rates in the identification problem.

4.1 SYSTEM ARCHITECTURE



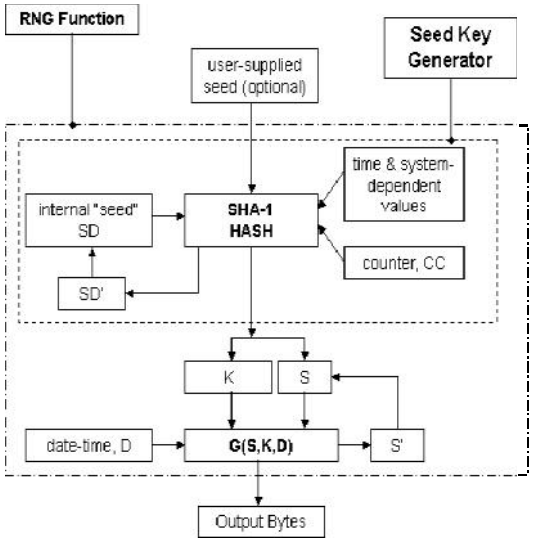
In mobile computing, collection of mobile nodes is connected at same access point. Initially all mobile nodes are registered and gets spread value called pseudo random number from base station. Mobile node broadcasting the packets through transmission channel and forward the packets to the base station. Then the base station verifies the spread value of certain mobile node along with user information which is retrieved from mobile data storage. The verification process is taken by GUIDE [17] algorithm .The base station blocks the packet if there is any mismatch between all the keying materials and detected as a replica node. Otherwise the base station identified that mobile node has the valid key materials. Then it encrypts the spread value before transferring the packets to transmission channel. Finally the transmission channel broadcast the packet.

4.2 GUIDE PROCESS

We proposed and evaluated metrics for resilience and delay which quantify the availability of control messages under control channel jamming attacks and demonstrated that the use of random key assignment provides graceful degradation in availability as the number of compromised user increases. We formulated the

identification of compromised users in the system as a maximum likelihood estimation problem and proposed the GUIDE algorithms using greedy heuristics for jammer identification and user identification. We provided an analytical approximation to evaluate the false alarm and miss rates in the identification of compromised users resulting from the GUIDE algorithms. We will investigate modifications to the adversary's jamming strategy and the effect on the availability of control messages and the ability to identify compromised users. Due to the complexity of the resulting identification problem, we propose technique, referred to as GUIDE (Greedy User IDEntification). This Technique has following methods to detect the replica node attack in mobile computing environment.

4.2.1 PSEUDO RANDOM NUMBER GENERATION



A pseudo-random number generator, or PRNG [18], is a random number generator that produces a sequence of values based on a seed and a current state. Random Number Generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. *Seed key* is a secret value used to initialize a cryptographic function or operation.

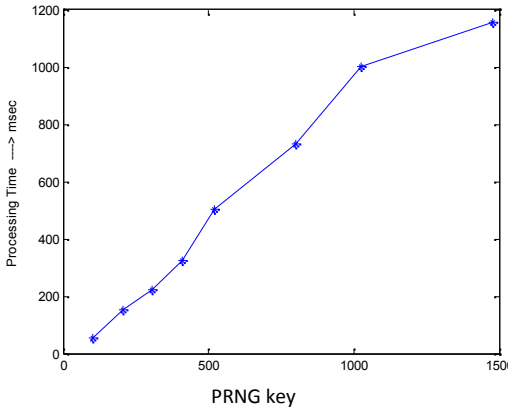
- CC, a 32-bit counter stored in thread-safe memory
- D, a 64-bit representation of the current date and time
- K, a 192-bit triple DES key
- L, a 64-bit value stored in thread-safe memory used to store the last value of X0
- P, a 64-bit value stored in thread-safe memory used to store the previously-generated block X
- S, a 64-bit generated seed value
- SD, a 64-bit value stored in thread-safe memory
- U, an optional user-supplied seed consisting of an arbitrary number of bytes

X, X0, X f, 64-bit generated values

The Secure Hash Algorithm is a one of cryptographic hash function SHA-1 is a 160 bit hash function which resembles the earlier MD5 algorithm.SHA-1 is employed in several widely used security application and protocols.

5 RESULTS

In the mobile replica cases, the mobile nodes IP address and its secret keying materials with the registered information in the base station are defined. Thus the results of replica node means the base station verified it as replica and block sending files. And also block its action, along with alarm information. If the mobile node has valid user information and key means, the base station allows broadcasting the packets in mobile computing environment. After verification of the specified mobile node, it will encrypt the key while forward it to the transmission channel. The following graph shows the relationship between the processing times of the mobile node and the PRNG key.



6. CONCLUSION

We have proposed a replica detection scheme for mobile networks based on the GUIDE (Greedy User IDEntification). We also generated random number to detect mobile replicas byusing the basic idea that a mobile node should never replicate anymore. Furthermore, we have presented two types of attacks that might be launched by the attacker and discussed the defence strategies against those attacks.

7 FUTURE ENHANCEMENT

Through the continuing investigation, that the architecture for better replica detection in mobile computing environment should be distributed and cooperative.For future work, we would like to thoroughly explore how localization and time synchronization errors affect the detection accuracy of our scheme.We would like to evaluate our scheme against various types of attacker models. In particular, we are interested in exploring how a variety of attacker models impact on the security of the scheme and also create one virtual memory to reduce the overload of base station.

8. REFERENCE

[1] D. Boneh and M.K. Franklin. Identity-Based Encryption from the Weil Pairing.In *Advances in Cryptology CRYPTO*, 2001.

[2] J-Y. L. Boudec and M. Vojnovi´c. Perfect Simulation and Stationary ofa Class of Moblity Models. In *IEEE INFOCOM*, 2005.

[3] J.B. Broch, D.A. Maltz, D.B. Johnson, Y-C.Hu, and J.G. Jetcheva.A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In *ACM MobiCom 1998*, October 1998.

[4] T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. *Wireless Communication and MobileComputing (WCMC): Special issue on Mobile Ad Hoc Networking:Research, Trends, and Applications*, 2(5):483-502, 2002.

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

[7] C. Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. In *the 8th IMA International Conference on Cryptographyand Coding*, 2001.

[8] M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei. A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks. In *ACM Mobihoc*, 2007.

[9] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. S. Sukhatme.Robomote: enabling mobility in sensor networks In*IEEE IPSN*, 2005.

[10] S. Ganeriwal, S. ˇCapkun, C.C. Han, and M.B. Srivastava. Secure timesynchronization service for sensor networks. In *ACM WiSe*, 2005.

[11] V. Gupta, M. Millard, S. Fung, Y. Zhu, N. Gura, S. Eberle, and H. Chang.Sizzle: A Standards-based End-to-End Security Architecture for theEmbedded Internet. In *IEEE International Conference on PervasiveComputing and Communications (PerCom)*, March 2005.

[12] L. Hu and D. Evans.Localization for Mobile Sensor Networks. In *ACM Mobicom*, 2004.

[13] J. Jung, V. Paxon, A.W. Berger, and H. Balakrishnan. Fast port detectionusing sequential hypothesis testing. In *IEEE Symposium on Security andPrivacy*, 2004.

[14] L. Lazos, S. ˇCapkun, and R. Poovendran. ROPE: Robust Position Estimation in Wireless Sensor Networks. In *IEEE International Conferenceon Information Processing in Sensor Networks (IPSN)*, April 2005.

[15] Z. Li, W. Trappe, Y. Zhang, and B. Nath. Robust Statistical Methodsfor Securing Wireless Localization in Sensor Networks.In *IEEEInternational Conference on Information Processing in Sensor Networks(IPSN)*, April 2005.

[16] A. Liu and P. Ning.TinyECC: A Configurable Library for EllipticCurve Cryptography in Wireless Sensor Networks. In *Technical ReportTR-2007-36, North Carolina State University, Department of Computer*

Science, November 2007.

[17]R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc., 2001

[18]Pietro, R., Mancini, L., and Mei, A. 2003. Random key assignment secure wireless sensornetworks. In 1st ACM workshop on Security of Ad Hoc and Sensor Networks.