Improved Bootstrapping Scheme with Cache Consistency for Invalidation Attack Resistance on MANET

P. Parameswari
ResearchScholar,
Anna University of Technology,
Coimbatore-641 047, India
param_pnr2000@yahoo.co.in

C. Chandrasekar
Associate Professor,
Periyar University,
Salem – 636 011, India
ccsekar@gmail.com

Abstract

Bootstrap protocol initiates neighbor node relationship and exchange knowledge information with other nodes in dynamic MANET. Security properties of Bootstrap protocol have need of an adversary effect undermine the correctness, and improvement in anticipation of an adversary. Our previous work presented an improved bootstrap security model with efficient cache consistency scheme to share proper and correct information sharing between the mobile nodes of the ad hoc network. Cache consistency scheme is a server control mechanism adapts the process of caching a data item and instructs the query node to updates data in the respective mobile cache nodes. In this paper, the proposed framework presents Secure Bootstrapping Scheme which uniformly operates as a good basis for new distributed bootstrapping scheme development in MANET to identify intrusion, damage recovery with cache consistency strategies. The proposal creates invalidation resistance techniques which identify frequently accessed data in which updates are pushed to its maximal. The multicast tree used for pushing cache invalidation and frequently accessed data to improve the system performance. The framework is common enough to hold existing schemes. This makes available us to compare these schemes according to a common base. In this paper, multicast tree built to validate the cached data with faster updates in ad hoc networks. Experiments are carried out with NS-2 simulator to show its effectiveness of restricting invalidation attack in terms of response time, attack resistance rate, false positive rate and Bandwidth.

Keywords: MANET, Bootstrapping, Cache Consistency, Invalidation Report

1. Introduction

The promise of enhanced security at the expense of open functionality is particularly appropriate in the context of mission-critical applications with the potential of an adversarial presence e.g., military Mobile Ad-hoc Networks (MANETs). It provided bootstrapping by which nodes form, the neighbor relationships among themselves in a manner consistent with current policy. However, this initial analysis neglected the possibility of nodes or wireless channel being subverted by a knowledgeable adversary. In MANET, data caching is essential as it reduces contention in the network, increases the probability of nodes getting desired data, and improves system performance. The major issue that faces cache management is the maintenance of data consistency between the client cache and the server.

All cache consistency algorithms are developed with the same goal in mind to increase the probability of serving data items from the cache that is identical to those on the server. A large number of such algorithms have been proposed in the literature, and they fall into three groups: server invalidation, client polling, and time to live (TTL). With server invalidation, the server sends a report upon each update to the client. Two examples are the Piggyback server invalidation and the Invalidation report mechanisms. In client polling, like the Piggyback cache validation of, a validation request is initiated according to a schedule. If the copy is up to date, the server informs the client that the data have not been modified; else the update is sent to the client. Finally, with TTL algorithms, a server-assigned TTL value (e.g., T) is stored alongside each data item d in the cache. The data d are considered valid until T time units pass since the cache update.

The proposed research will study methods to avoid or detect malicious nodes via authentication mechanisms. Proposed secure bootstrapping scheme for MANETs is policy-neutral because it distills mechanisms from policies, under which users are admitted. This means that our framework hold a large class of policies. With this approach, the data sources sign the data with its private key, so that intermediate routers cannot modify the data. In this research, we design and evaluate techniques to reduce such overhead and balance system performance and security strength. Further, we identify possible security attacks on cache consistency and propose viable mechanisms to defend against such attacks.

2. Related Works

A crucial challenge in a deny-by-default mission critical MANET, in which network topology and information exchange requirements can be time-varying, is the manner in

ISSN : 2349 - 6363

which the nodes maintain up-to-date policy [1]. Our previous work addressed this challenge by defining (i) an axiomatic set of policies from which nodes can obtain additional policies or update outdated policies and (ii) a protocol (referred to as the Bootstrap protocol) by which nodes form, or bootstrap, the neighbor relationships among themselves in a manner consistent with current policy. Along with the definition of the Bootstrap protocol as a Finite State Machine (FSM) [2], we also proved its correctness (safety and liveness), however, this initial analysis neglected the possibility of nodes or wireless channel being subverted by a knowledgeable adversary.

Several cache consistency (invalidation) schemes have been proposed in the literature [3], [4] for MANETS. In general, these schemes [5], [6] fall into three types i.e., pull or client model (caching node (CN) asks for updates from server), push or server model, (server sends updates to CN), and cooperative model (CN and server cooperate to keep the data up-to-date). Pull-based strategies [7] achieve smaller query delay times at the cost of higher traffic load, whereas push-based strategies achieve lower traffic load at the cost of larger query delays. Cooperative-based strategies [8] tend to be halfway between both ends.

Recently, many researchers start to look into security issues in ad hoc networks. In [13] addressed the issues of distributing public keys in ad hoc networks, by proposing to let users issue certificates for each other based on their personal acquaintances. In [10] proposed a solution based on threshold cryptography. Based on a trusted certificate authority, the authors of [9], [15] proposed a solution to secure the routing protocol of ad hoc wireless networks. To address the high overhead associated with obtaining and verifying the digital certificates, in [11] proposed a protocol to secure on-demand routing protocols based on TESLA [14], an efficient broadcast authentication scheme that requires loose time synchronization. They also identified the wormhole attack [12], which may make most routing protocols unable to find routes longer than one or two hops. Based on the intuition that a receiver can determine if the packet has traversed a distance that is unrealistic with precise timestamp or location information, they provided a packet leash solution to solve the wormhole attack.

3. Improved Bootstrapping Scheme with Cache Consistency for Invalidation Attack Resistance on MANET

A MANET is formed on-the-fly to accomplish some task. Therefore, it would be reasonable to assume that some initiators would bootstrap a MANET by admitting outside users according to a predetermined policy, denoted by policy, and by issuing some cryptographic credentials to the admitted users. The bootstrap protocol allows the two nodes to establish a neighbor relationship when that relationship, and the process for bootstrapping that relationship, is consistent with policy. All messages (exchanged between two nodes) are privacy and integrity protected via encryption and cryptographic hash. Strong identity (e.g., provided by signature) is in place, so no node can impersonate any other node. Each message has a timestamp, which serves as a sequence number for defending against message reordering/replaying attack. Node never simultaneously keeps two or more bootstrap sessions with any other node.

3.1 Secure bootstrapping Communication in MANET

The secure bootstrapping scheme takes already existing authenticated (private) channels between two users when they are surrounded by a short distance of each other. When authenticated private channels be present, the final outcome is more efficient than the ones that are exclusively depends on authenticated channels. Communications are achieved entirely over the afore-discussed authenticated channels, or partially over them due to their potentially narrow bandwidth in which there are only used to create common cryptographic keys that are then used to keep the communications over the ordinary wireless channels. This operation of mobility for security is convenient because physical attendance is perhaps the most excellent way to amplify joint trust and to exchange information in a secure way, particularly in the environment of MANETs.

3.2 Secured Cache consistency scheme

The cooperative cache adopts a widely accepted system model in which each data object is associated with a single node that can update the source data. Each data object can be cached by a collection of nodes called the caching nodes. The data copies held by the caching nodes are called the cache copies. There are two basic mechanisms for cache consistency maintenance i.e., push and pull. Using push, the data source node informs the caching nodes of data updates. Using pull, the caching node sends a request to the data source node to check the update. In designing cooperative cache the source data updates and the cache queries follow the Poisson Process. The routing protocol employed in the network layer provides the hop count between each pair of nodes, and the hop count of data transmission is used to measure the consistency maintenance. The consistent server cache updates provides data Consistency based on the Pull with TTR. Although the Pull with TTR algorithm guarantees data Consistency, it is not cost effective, mainly due to the round–trip consistency maintenance cost imposed by the pull mechanism.

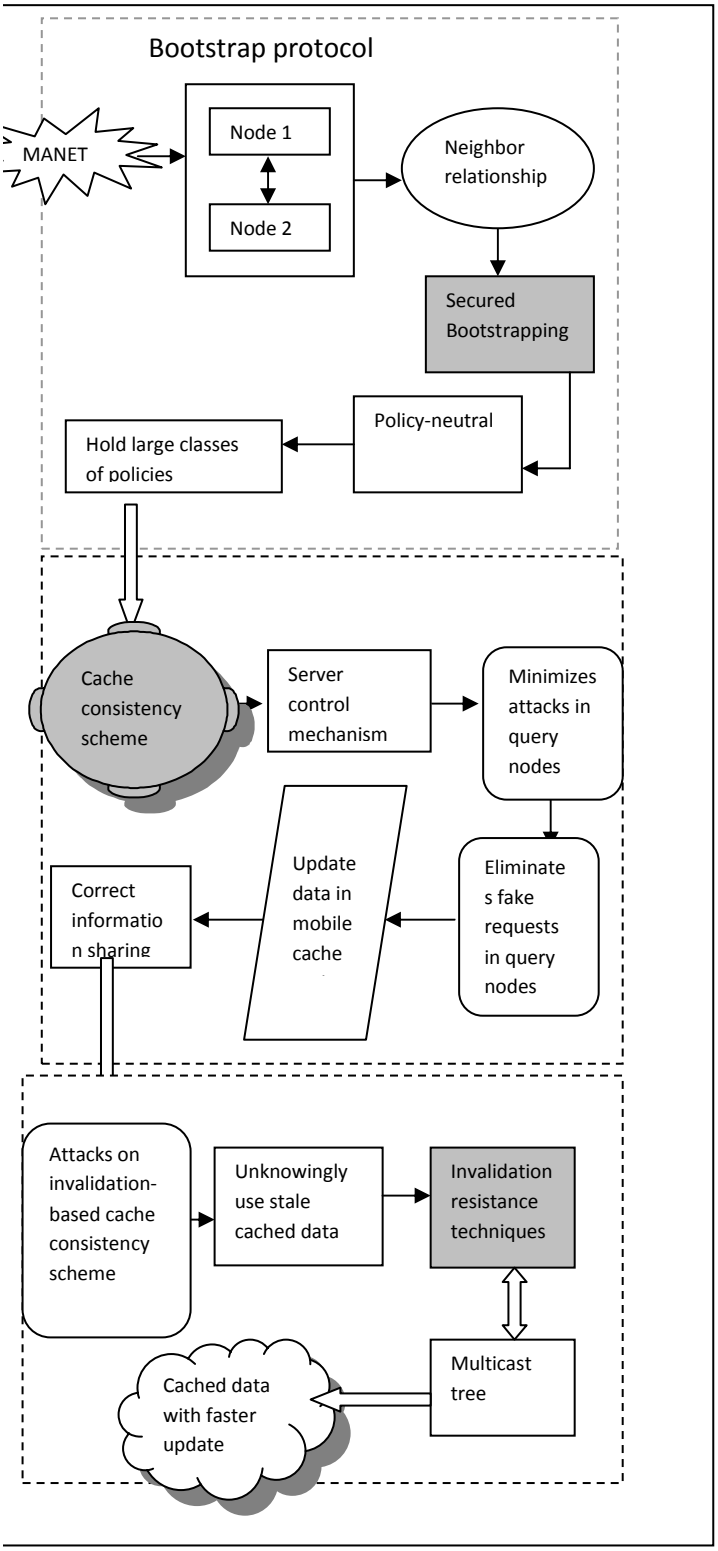

Figure 1: Improved Bootstrapping Scheme with Cache Consistency for Invalidation Attack Resistance on MANET

3.3 Adversarial model

Hybrid adversarial model is considered in which the adversary cannot break any cryptographic scheme that is proven secure in the modern cryptography framework. Moreover, the adversary cannot break the source identification and channel integrity of an assumedly authenticated channel; or, the adversary cannot break the source identification, channel integrity, and channel confidentiality of an assumedly authenticated private channel. From a system security perspective, the adversary may be able to capture some users who are within a short distance of it, and then take out their secrets (e.g., cryptographic keys) stored on their devices. This means that the malicious and capable owner of a hardware module always has compromised it, and that the resulting damage (e.g., compromise of data confidentiality due to the compromise of cryptographic keys) must be handled at a higher layer of attack-resilience management.

3.4 Invalidation Attacks

Adversary acting as an initiator, In the setting of distributed bootstrapping of MANETs, the initiators does not know in advance are the users that will be admitted are and the users also do not know about the initiators. The objective of the adversary is to disrupt the establishment of security relations between users that are admitted into a MANET that is bootstrapped by some trusted initiators. We consider two types of attacks that a malicious node can launch on the invalidation-based cache consistency scheme. First one, the node may drop some invalidation messages, such that its descendants can not receive the message and hence may unknowingly use stale cached data. Second, the node may modify some invalidation messages that it forwards, such that its descendants may receive wrong invalidation messages and hence may unknowingly use stale cached data or unnecessarily invalidate cached data.

3.5 Invalidation Attack Resistance with faster cache updates and consistency

We consider a wireless ad hoc network, which consists of a data center and many ordinary nodes. The data center (also called server) stores data that is updated now and then.

Some ordinary nodes (called clients) frequently access the data, and cache some data locally to reduce network traffic and data access delay. We assume strong cache consistency is required, and the invalidation based bootstrapping and cache consistency model is used. In the invalidation-based scheme, the server control node needs to send invalidation messages to clients. The most reliable method to ensure that all co-operative neighbor nodes with cached data, receive the invalidation messages is to use flooding, which has very high overhead. The invalidation resistance techniques identify

frequently accessed data in which updates are pushed to its maximal. It is easy to see that the multicast tree can be used for pushing cache invalidation and frequently accessed data to improve the system performance. In this paper, we assume that a multicast tree has been built to validate the cached data with faster updates in ad hoc networks.

4. Performance Evaluation

Experimental simulations are conducted with NS-2 (V2.34) to evaluate the control packet, message delivery rate and end to end delay of the bootstrapping security mechanism applied. The simulation used a random way point model, area 1000 * 1000, maximum velocity 20 m/s, wireless range 250 m, nodes 50, and data transfer rates 4packets/s for our simulation topology scenarios. Each run of the simulator accepts a scenario file as input that describes the exact motion of each node and the exact sequence of packets originated by each node, together with the exact time at which each change occurs in motion or packet origination. Since each protocol was changed in an identical fashion, the performance of these protocols can directly be compared.

The experimentation is conducted on the MANET for evaluating the security scheme in terms of attack resistance rate, false positive rate, and bandwidth and query response time. These are the differences between the corresponding measures when no cache updating is in place and when server update mechanism is employed. Requests for data in the ad hoc network and data updates at the server are assumed to be random processes and may be represented by exponential random variables. The rate of requests processing depends on the fastness of rate of updates.

5. Results and Discussion

The efficiency of proposed Secured Bootstrapping Scheme is evaluated compared with the unsecured bootsrapping Scheme. The performance metrics are Attack Resistance Rate, False Positive Rate, Bandwidth and Query Response Time. Both the bandwidth metric and response time metric are influenced by the number of data requests issued by requesting nodes relative to the number of data updates that occur at the server.

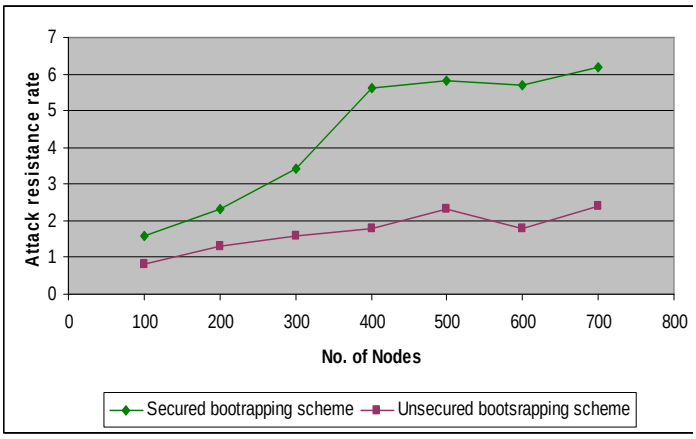

Figure 2: Number of nodes Vs Attack resistance rate

Figure 2 shows the attack resistant rate of Secured Bootstrapping Scheme with number of nodes The security resistance performance (fig 2) generates a reasonable trade-off, especially when number of nodes is sacrificed in order to speed up the query response time. Secured Bootstrapping Scheme achieves the better performance.

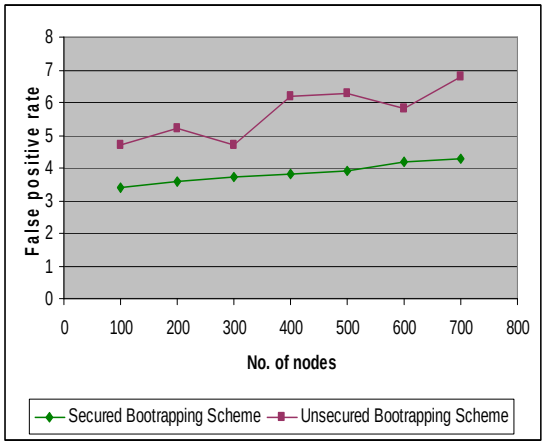

Figure 3: Number of nodes Vs False positive rate

Figure 3 shows Number of nodes Vs False positive rate. In this we found Secured Bootstrapping Scheme decreases the false positive rate compared with the unsecured Bootstrapping Scheme. As the number of nodes increases, false positive rate also gets increased. The Secured Bootstrapping Scheme is having the efficient false positive rate.

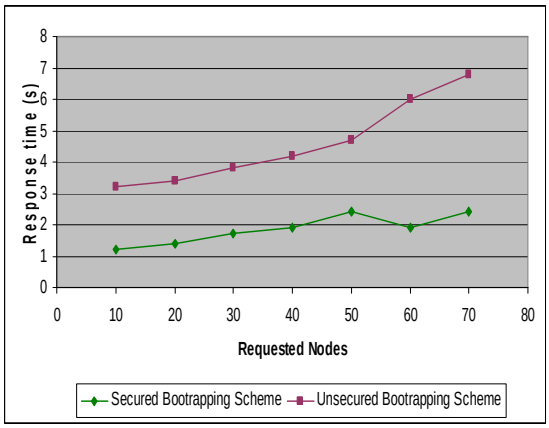

Figure 4: Requested nodes Vs Response time

Figure 4 depicts the response of Secured Bootstrapping Scheme with number of nodes. Secured Bootstrapping Scheme speeds up the query response time. So it takes less time to respond the Query.

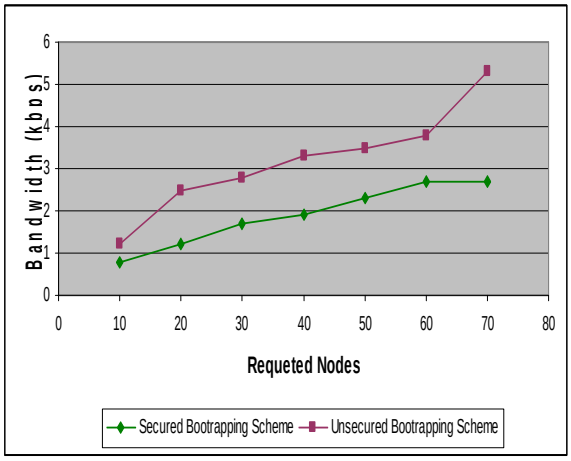

Figure 5: Requested nodes Vs Bandwidth

Fig 5 shows that the bandwidth utilization per node increases with the UnSecured Bootstrapping Scheme, but in Secured Bootstrapping Scheme minimum bandwidth utilization is required which shows better performance of our proposed work.

6. Conclusion

We have implemented Secured Bootstrapping Scheme for mobile ad-hoc networks. Fake requests in query nodes have been eliminated. The Scheme is policy neutral, and holds existing bootstrapping schemes. The implemented Secured Bootstrapping Scheme acheived intrusion detection, damage recovery and intruder identification using bootstrapping and cache consistency strategies. When caching techniques are used, cache consistency issues must be addressed. The invalidation-based approach is widely used to maintain strong cache consistency. However, this approach may suffer from some security attacks. Our proposed technique used to restricting the invalidation attack on bootstrapping and cache consistency. The experimentation is conducted with NS-2 simulator and showed improved attack resistance rate, false positive rate, Bandwidth and Response time

References

[1] ShouhuaiXu, SrdjanČapkun, “Distributed and Secure Bootstrapping of Mobile Ad Hoc Networks: Framework and Constructions”, ACM Transactions on Information and Systems Security, Vol. 12, No. 1,2008.

[2] H. Ballani, Y. Chawathe, S. Ratnasamy, T. Roscoe, and S. Shenker.“Off by default!” in HotNets-IV, November 2005.

[3] M. Bauer, “Paranoid penguin: Introduction to selinux, part ii”, Linux Journal, vol. 155, 2007.

[4] S. Bratus, A. Ferguson, D. McIlroy, and S. Smith, “Pastures: Towards usable security policy engineering,” in 2nd International Conference onAvailability, Reliability and Security, 2007.

[5] H. Peine, “Rules of thumb for developing secure software: Analyzing and consolidating two proposed sets of rules,” in 3rd Int. Conf. onAvailability, Reliability and Security, 2008.

[6] T. Wolf, “Design of a network architecture with inherent data path security,” in 3rd ACM/IEEE Symposium on Architecture for networkingand communications systems, 2007.

[7] M. Srivatsa, D. Agrawal and S. Balfe, "Bootstrapping Coalition MANETs" in ITA Technical Report, February 2008.

[8] H. Artail and K. Mershad, “MDPF: Minimum Distance Packet Forwarding for Search Applications in Mobile Ad Hoc Networks,” IEEE Trans. Mobile Computing, vol. 8, no. 10, pp. 1412- 1426, Oct. 2009.

[9] O. Bahat and A. Makowski, “Measuring Consistency in TTLBased Caches,” Performance Evaluation, vol. 62, pp 439-455, 2005.

[10] J. Cao, Y. Zhang, L. Xie, and G. Cao, “Consistency of Cooperative Caching in Mobile Peer-to-Peer Systems over MANETs,” Proc. Third Int’l Workshop Mobile Distributed Computing, vol. 6, pp. 573- 579, 2005.

[11] D. Zhou and T.H. Lai, “An Accurate and Scalable Clock synchronization Protocol for IEEE 802.11-Based Multihop Ad Hoc Networks,” IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 12, pp. 1797-1808, Dec. 2007.

[12] H. Jin, J. Cao, and S. Feng, “A Selective Push Algorithm for Cooperative Cache Consistency Maintenance over MANETs,” Proc.Third IFIP Int’l Conf. Embedded and Ubiquitous Computing, Dec. 2007.

[13] W. Li, E. Chan, Y. Wang, and D. Chen, “Cache Invalidation Strategies for Mobile Ad Hoc Networks,” Proc. Int’l Conf. Parallel Processing, Sept. 2007.

[14] X. Yang, D. Wetherall, and T. Anderson, “A DOS-limiting network architecture,” in ACM SIGCOMM, 2005.