Design and Implementation of Enhanced Secure Field Based Routing in Wireless Mesh Network (WMN)

Sanjaya Kumar Sen[1], Riyazuddin Khan[2]

[1]Professor, Einstein Academy of Technology & Management, Bhubaneswar
[2]Associate Professor, Einstein Academy of Technology & Management, Bhubaneswar

Abstract

In many mission critical applications such as troop coordination in a combat field, situational awareness etc. wireless mesh networks are becoming an effective tool. These applications are served by and use the multicast-style of communication traffic. Therefore, authenticating the source and ensuring the integrity of the message traffic become a fundamental requirement for the operation and management of the network. However, the limitation of computation and communication resources, in a large scale deployment and the unguaranteed connectivity to trusted authorities make even the known solutions for wired and single-hop wireless networks inappropriate.
This project presents an authentication scheme for multicast traffic for wireless mesh network where it combines the advantages of the time asymmetry and the secret information asymmetry paradigms and exploits network clustering to reduce overhead and ensure scalability. Multicast traffic within a cluster employs a one-way hash function chain in order to authenticate the message source. Cross-cluster multicast traffic includes message authentication codes (MACs) that are based on a set of keys. Each cluster uses a unique subset of keys to look for its distinct combination of valid MACs in the message in order to authenticate the source. The results aims to show greater security to the sender and as well as to the message and to the destination.

***Keywords**:* Wireless mesh networks; Multicast communications; Message authentication

1. Introduction

The main topological characteristic of Wireless Mesh Network (WMN) is that there is only one or several node connecting to the infrastructure network as gateway and all other nodes connect to the gateway through the relay of the neighboring nodes, and then connect with the internet. WMN represents a whole new network concept and because of the nature of wireless and multi-hop, the security vulnerabilities have become crucial problems. In secure field based routing approach - route the packet securely from gateway to the network. To route a packet Field based routing is used. It uses a little information to route the packets in the network. Due to this characteristic, field based routing algorithms are less expensive and much effective, but such algorithms also face different types of security attacks.

Cross-cluster multicast traffic includes message authentication codes (MACs) that are based on multiple keys. Each cluster looks for a distinct combination of MACs in the message in order to authenticate the source. The source generates the keys at the time of establishing the multicast session. The keys will be securely transmitted to the head of every cluster that hosts one or multiple receivers. The multicast message is then transmitted to the cluster-heads which authenticate the source and then deliver the message to the intended receivers using the intra-cluster authentication scheme.

The rationale is that the MAC will be associated with the cluster rather than the nodes and thus the overhead is reduced significantly. Group communication is considered a critical service in wireless mesh networks due to their inherently collaborative operations, where the nodes cooperate in network management and strive to accomplish common missions autonomously in highly unpredictable environment without reliance on infrastructure equipment. For example, in combat missions troops report their status and share observed data in order to become aware of the overall situation and coordinate their actions. In addition, it is common for wireless mesh network to rely on multicast for management-related control traffic such as neighbor/route discovery to setup multi-hop paths, the establishment of time synchronization, etc. Such multicast traffic among the nodes has to be delivered in a secure and trusted manner. In particular the provided network services need to achieve the following security goals: (1) Confidentiality, to prevent adversaries from reading transmitted data, (2) Message integrity, to prevent tampering with transmitted messages, and (3) Source Authentication, to prevent man-in-the-middle attacks that may replay transmitted data for node impersonation. Confidentiality is achieved by encrypting the transmitted data. The work presented in this project aims at addressing the second and third goals. Providing an efficient multicast message and source authentication security service that can easily scale for large networks is an important capability for the operation and management of the underlying network. Source and message authentication is the corroboration that a message has not been changed and the sender of a message is as claimed to be. This can be done by sending a (1) Cryptographic digital signature, or (2) Message Authentication Code (MAC) . The first involves asymmetric cryptography and often needs heavy computation both at the sender and the receiver. The latter involves creating a message and source specific MAC that can be verified by the receiver. Thus, the MAC implicitly ensures message and source integrity.

In unicast, a shared secret key is used for MAC generation. Unfortunately, the use of a single shared key in multicast makes the group vulnerable to source impersonation by a compromised receiver. Dealing with multicast as a set of unicast transmissions each with a unique shared key is the most inefficient approach for addressing this concern. These issues combined with other constraints have made contemporary message and source authentication schemes used for multicast traffic in wired and single-hop wireless networks unsuitable for mesh networks.

To meet its requirements, WMN technology contains several characteristics such as:

- ***Multi-hop operation***: WMN is a technology of rupture that aims to avoid having sensitive points, which in case of breakdown, cut the connection from part of the network. So, if a host is out of service, its neighbors will pass by another path.
- ***Capability of self-forming, self-healing, and self-organization***: WMN solutions authorize a fast and simplified deployment, a great extension of the coverage and, by their architecture, a strong fault-tolerance for interference and breakdowns. This tends to reduce costs of installation and exploitation of networks.
- ***Station Mobility:*** Clients, in WMN, are by definition mobile. Therefore, they expect to have a continuous connection to their network services. Processes, such as authentication and association, must be done transparently.
- ***Compatibility and interoperability with existing networks:*** Mesh networks offer the possibility to coexist with existing networks which have other architectures and numerous characteristics that may be different from those of WMN. Indeed, the gateway WMR allows the establishment of connection between WMN and Internet.
- ***Unconstrained power-consumption:*** Mesh routers have a permanent source of power so they do not have strict constraints on power consumption. However, clients in WMN necessitate the installation of power efficient.

2. Challenges and Design Goals

Multiple factors make multicast authentication in mesh networks very challenging. The issues are fundamentally due to the resource constraints and the wireless links. First, nodes have limited computing, bandwidth, and energy resources which make the overhead of basic asymmetric key-pair cryptography methods very expensive. In addition,

the unstable wireless links due to radio interference cause frequent packet loss errors and require a security slution that can tolerate missed packets, as well as differentiate between packet retransmission and replay. Furthermore, the instability of the wireless links makes it unwise to rely on the continual involvement of a trusted authority in the generation and sharing of session keys since a stable connection cannot be guaranteed. On the other hand, while basic symmetric key cryptography methods are efficient, they are ineffective for multicast traffic patterns since using a common key for all receivers will make it relatively easy to impersonate a sender by any of the receiving nodes.

In addition to being resource efficient and robust to packet loss, a security solution should scale for large group of receivers and long multi-hop paths. Thus, a solution that is based on a distinct authentication key for every receiver will introduce prohibitive overhead to the message and consume significant portion of the available bandwidth. Moreover, the solution should scale for large number of senders by requiring reasonable memory resources at the individual receivers for storing authentication keys. Finally, it is desired to enable the validation of every packet without excessive delay and independent of the other packets. This goal would affect when the authentication code of a packet will be sent and how sensitive the security scheme will be to an occasional delay or

a loss of some packets. The motive is that some data may be urgent, e.g. a report on an enemy tank, and should be acted upon as soon as possible, and thus the authenticity of the source should be verified rapidly.

This project proposes Authentication scheme for Multicast traffic for ad-hoc networks. It exploits network clustering in order to cut overhead and ensure scalability. Multicast traffic within the same cluster employs one-way hash chains to authenticate the message source.

The authentication code is appended to the message body. However, the authentication key is revealed after the message

is delivered The relatively small-sized cluster would make it possible to keep the nodes synchronized and address the maximum variance in forwarding delay issue of message authentication within a cluster. On the other hand, cross-cluster multicast traffic includes message authentication codes (MACs) that are based on multiple keys. Each cluster looks for a distinct combination of MACs in the message in order to authenticate the source.

The source generates the keys at the time of establishing the multicast session. The keys will be securely transmitted to the head of every cluster that hosts one or multiple receivers. The multicast message is then transmitted to the cluster-heads which authenticate the source and then deliver the message to the intended receivers using the intra-cluster authentication scheme. thus combines the advantages of the secret information asymmetry and the time asymmetry paradigms

3. RELATED WORK

Source authentication schemes found in the literature can be classified into three categories: (1) secret information asymmetry, (2) time asymmetry, and (3) hybrid asymmetry The asymmetry property denotes that a receiver can verify the message origin using the MAC in a packet without knowing how to generate the MAC. This property is the key for preventing impersonation of data sources. In secret information asymmetry every node is assigned a share in a secret, e.g., a set of keys. A source appends MACs for the multicast keys so that a receiver verifies the authenticity of the message without being able to forge the MACs for the other nodes. The challenge in using this category of approaches is striking the balance between collusion resilience and performance impact. While the use of a distinct MAC per node imposes prohibitive bandwidth overhead, relying on the uniqueness of the key combinations risks susceptibility to node collusion. It pursues secret information asymmetry for its inter-cluster operation and limits the key pool size to suit only the number of clusters.

The main idea behind time asymmetry is to tie the validity of the MAC to a specific duration so that a forged packet can be discarded. One-way hash chains are usually employed to generate a series of keys so that a receiver can verify the current key based on an old key without being able to guess the future key. Initially, a source picks a key K0 and generates a chain of keys by recursively applying a one-way hashing function. These keys are used to form the MAC for the individual data packets. The source then reveals the last key, *Kl*, in the chain to all receivers to serve as the baseline for verification. The key which is used to generate the MAC of a packet is revealed after some time period so that the key cannot be used to impersonate the source. When revealed, the receiver validates the key using *Kl* or any of the previously revealed keys.

One of the most distinct advantages of time asymmetry is the minimal per packet overhead that they impose. However, it requires clock synchronization among the communicating parties in order to prevent accepting forged packets, or discarding authentic packets. In addition, in large networks, forwarding delay will force the node to limit the packet transmission rate to avoid revealing next keys to intermediate nodes before all receivers get all previously transmitted packets. These shortcomings limit the scalability of these approaches for multi-hop networks where the maximum end-to-end delay varies significantly among receivers over time and space due to congestions and topology dynamics. Although, some attempts have been made to limit the impact of these issues, the scalability of time asymmetry approaches is still questionable.

Each group is pre-assigned a leader to act as a trust authority. The group leader is responsible for multicasting commands to group members and interfacing its group to other groups in the network...

4. Architectural Model

In the mesh network is a collection of autonomous nodes that together set up a topology without the support of a physical networking infrastructure. Depending on the applications, a mesh network may include up to a few hundreds or even a thousand nodes. Communications among nodes are via multihop routes using Omni directional wireless broadcasts with limited transmission range. In the system model considered in this project, nodes are grouped into clusters. The clusters formation can be based on location and radio connectivity. It is assumed that clusters are established securely by using pre-distributed public keys , employing a robust trust model , or applying identity based asymmetric key-pair cryptographic methods, and that a proper key management protocol is followed in order to perform reclustering when needed. Clustering is a popular architectural mechanism for enabling scalability of network management functions. It has been shown that clustered network topologies better support routing of multicast traffic and the performance gain dominates the overhead of creating and maintaining the clusters.

Each cluster is controlled by a cluster-head, which is reachable to all nodes in its cluster, either directly or over multi-hop paths. Nodes that have links to peers in other clusters would serve as gateways. The presence of gateways between two clusters implies that the heads of these clusters are reachable to each other over multi-hop path and that these two clusters are considered neighbors. If a node moves out its current cluster and joins another, it is assumed that the associated cluster-heads will conduct a handoff to update each other about the change in membership of their clusters; other cluster-heads will not be involved in the handoff events outside their clusters. Mobility is not the focus of this project; however, prior studies have shown that clustering is advantageous for multicast routing in mobile environments.

We aim to eliminate any need for interaction with the authority to retrieve the public key of some nodes in the network. The source uses asymmetric cryptography to deliver the session keys to the main players in the authentication process. All nodes are to be preloaded with a known one-way hash cryptographic function. The function should be proven secure with extremely low probability that an adversary can determine the input to the function given its output.

This project mainly considers an adversary who tries to manipulate the system through capturing and compromising some nodes. When a node is captured, its memory can be read or tampered with. Therefore, an adversary would know the keys of a compromised node. In addition, the operation of a compromised node may be manipulated to launch attacks such as replay, impersonation, etc.

5. Proposed System

I am going to develop an Authentication scheme for Multicast traffic for large scale dense mesh networks. It combines the advantages of the time asymmetry and the secret information asymmetry paradigms and exploits network clustering to reduce overhead and ensure scalability. multicast traffic within a cluster employs a one-way

hash function chain in order to authenticate the message source. Cross-cluster multicast traffic includes message authentication codes (MACs) that are based on a set of keys. Each cluster uses a unique subset of keys to look for its distinct combination of valid MACs in the message in order to authenticate the source.

The asymmetry property denotes that a receiver can verify the message origin using the MAC in a packet without knowing how to generate the MAC. This property is the key for preventing impersonation of data sources.

Advantages:

- ✓ Securing such traffic is of great importance, particularly authenticating the source and message to prevent any infiltration attempts by an intruder.
- ✓ Both time and secret-information asymmetry in order to achieve scalability and resource efficiency

6. CONCLUSION

In recent years there has been a growing interest in the use of mesh networks in security-sensitive applications such as digital battlefield, situation awareness, and border protection. The collaborative nature of these applications makes multicast traffic very common. Securing such traffic is of great importance, particularly authenticating the source and message to prevent any infiltration attempts by an intruder.

Contemporary source authentication schemes found in the literature either introduces excessive overhead or do not scale for large networks. This project has presented combining both time and secret-information asymmetry in order to achieve scalability and resource efficiency. The performance has been analyzed mathematically and through simulation, confirming its effectiveness. In addition, the effect of the various parameters has been studied and guidelines have been highlighted for picking the most suitable configuration in the context of the particular application requirements; most notably having a cluster radius of 2 or 3 hops appears to be the most suitable for this project. Our future work plan includes studying the effect of different clustering strategies on the performance.

In this project, to allow the users an effective and reliable handoff, as well as a secure access to the mesh network through an authentication mechanism should be executed during the mobility of the mobile nodes over a different and through various clusters. Indeed, the routing with authentication cannot prove its effectiveness only if it is associated to a well-defined and studied security mechanism. In addition, a WMN can be prone to many types of attacks.

The success of these kind of attacks based on the hidden identify of the intruders. That is why having knowledge about the entire path of attacks packets can be helpful in making defensive decisions. In this project, the proposed new solution deals with the problem of insecurity, during the hands-off of the message to the destination nodes, with encryption/decryption and using the MAC key for each message.

REFERENCE

[1] Fahad T. Bin Muhaya1, 2, Fazl-e-Hadi2 and Atif Nasser on ESFBR- Enhanced secure field based routing in wireless mesh networks, Indian Journal of Science and Technology- 2011
[2] M Faouzi Zarai, Ikbel Daly, and Lotfi Kamoun on Security in Wireless Mesh Networks International Journal of Computer Network and Security (IJCNS) Vol. 3 No. 1
[3] A Gerkis on A Survey of Wireless Mesh Networking Security Technology and Threats
[4] A. Perrig, R. Canetti, D. Song, and D. Tygar, “Efficient authentication and signing of multicast streams over lossy channels,” in Proc. 2000 IEEE Symposium Security Privacy.
[5] R. Canetti et al., “Multicast security: a taxonomy and efficient constructions,” in Proc. 1999 IEEE INFOCOM
[6] Perrig, et al., “Efficient and secure source authentication for multicast,” in Proc. 2001 Network Distributed System Security Symposium
[7] C. E. Perkins, Ad Hoc Networking. Addison-Wesley, 2001.

[8] H. Yang, et al., "Security in mobile ad-hoc wireless networks: challenges and solutions," IEEE Wireless Commun. Mag., vol. 11, no. 1, pp. 1536– 1284, Feb. 2004.
[9] Y. Challal, H. Bettahar, and A. Bouabdallah, "A taxonomy of multicast data origin authentication, issues and solutions," IEEE Commun. Surveys & Tutorials, vol. 6, no. 3, pp. 34–57, 2004.
[10] A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient authentication and signing of multicast streams over lossy channels," in Proc. 2000 IEEE Symposium Security Privacy.
[11] R. Canetti et al., "Multicast security: a taxonomy and efficient constructions," in Proc. 1999 IEEE INFOCOM.
[12] R. Safavi-Naini and H. Wang, "Multi-receiver authentication codes: models, bounds, constructions, and extensions," Inf. Computation, vol. 151, no. 1–2, pp. 148–172, May 1999.
[13] Perrig, et al., "Efficient and secure source authentication for multicast," in Proc. 2001 Network Distributed System Security Symposium.
[14] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," in Proc. 2001 ACM Conf. Computer Commun. Security.
[15] Wireless Mesh Networking: Architectures, Protocols and Standards (Wireless Networks and Mobile Communications,Yan Zhang,Jijun luo.
[16] M. Mosko and J. J. Garcia-Luna-Aceves, "Ad hoc routing with distributed ordered sequences," in IEEE INFOCOM 2006, Barcelona, Spain, April 2006.
[17] H. Ju and I. Rubin, "Backbone topology synthesis for meshed wireless LANs," in IEEE INFOCOM 2006, Barcelona, Spain, April 2006.
[18] M. Mosko and J. Garcia-Luna-Aceves, "Multipath routing in wireless mesh networks," in Proc. IEEE Workshop on Wireless Mesh Networks (WiMesh), Santa Clara, USA, sep 2005.
[19] Power-aware dual-tree-based multicast routing protocol for mobile ad hoc networks by N.-C. Wang, Department of Computer Science and Information Engineering, National United University, Miao-Li 360, Taiwan.
[20] The Development of Localized Algorithms in Wireless Sensor by Networks Hairong Qi*, Phani Teja Kuruganti and Yingyue Xu .
[21] Z. J. Haas and M. R. Pearlman, "The performance of query control schemes for the zone routing protocol," in SIGCOMM, 1998, pp. 167– 177.
[22] J.-C. Chen and S. Li and S.-H. Chan and J.-Y. He, "WIANI: Wireless Infrastructure and Ad-Hoc Network Integration," in Proceedings of IEEE.
[23] Review On Routing Algorithms In Wireless Mesh Networks(K.P. Vijayakumar1, P. Ganeshkumar2 And M. Anandara) International JournalOf Computer Science And Telecommunications [Volume 3, Issue 5, May 2012].