International Journal of Information Technology and Management

Vol. VII, Issue No. X, November-2014, ISSN 2249-4510

AN EVALUATION OF VARIOUS ROUTING SECURITY FOR MOBILE AD-HOC NETWORKS: A CASE STUDY OF ROBUST UBIQUITOUS SECURITY SUPPORT SYSTEM

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VII, Issue No. X, November-2014, ISSN 2249-4510

An Evaluation of Various Routing Security for Mobile Ad-Hoc Networks: A Case Study of Robust Ubiquitous Security Support System

Dr. Shailendra Singh Sikarwar[1] Mahesh Bansal[2]

[1]Assistant Professor, P. G. V. College, Gwalior

[2]Assistant Professor, P. G. V. College, Gwalior

Abstract – Mobile ad hoc networks are infrastructure-free, pervasive, and ubiquitous and without any centralized authority. These unique characteristics, combined with security threats, demand solutions in securing ad hoc networks prior to their deployment in commercial and military applications. So far, the research in mobile ad hoc network has been primarily focused on routing and mobility aspects rather than securing the ad hoc network itself. Due to the ever-increasing security threats, there is a need to develop algorithms and protocols for a secured ad hoc network infrastructure. This paper surveys the prevailing mobile ad hoc network security threats and the existing solution schemes.

Current technologies and security advances have made networked systems and applications very popular and widely used. The pen asive and practical aspects of wireless Mobile Ad Hoc Networks (MANET) made them very popular as well. This created the need for securing MANETs to provide users with authentic communications, secure and robust information exchange, and efficient security mechanisms. However, many of the security solutions devised for regular networks are not as efficient nor as effective on MANETs. This paper investigates the security issues of a common type of MANETs (open/dynamic VIANET) at the network layer -where routing protocols and forwarding mechanisms are used. In this paper, we identify the different security requirements specific to MANETs and sun ey some of the available secure routing techniques. The study has rep ealed some problems with the current routing protocols and identified the most important issue that needs to be resolved to ensure a secure network layer.

In our design, we distribute the functions of the certification authority through a threshold secret sharing and scalable multi-signature mechanism, in which each node holds a secret share and multiple nodes in a local neighborhood jointly provide complete services. Localized certification schemes are devised to realize ubiquitous service availability. We also update the secret shares to further enhance robustness against break-ins.

----------♦----------

INTRODUCTION

Computer networks are a living necessity for almost everybody. However, they also have generated the need for sophisticated and robust security mechanisms to protect them and many have been successful in conventional networks. Currently, new technologies have emerged in the context of wireless connectivity, which are becoming popular for applications such as home and office networking and connecting mobile users. With this advancement, the need for security has also elevated, generating more research to secure wireless networks.

One of the important types of wireless networks is the infrastructure less (ad hoc) network. These networks do not have a fixed topology and do not need a centralized server to operate correctly. Ad hoc networks allow independent nodes to communicate autonomously and rely on the nodes to perform network functions such as routing and security. To add to the complexity, nodes are usually heterogeneous with varying and limited resources and are mobile. This creates the need for efficient and fast mechanisms to facilitate the connections and to provide secure routing services, hi ad hoc networks, security becomes essential and complicated. Security protocols and algorithms that were used and proven in regular networks 110 longer satisfy the requirements in MANET. The unique characteristics of MANETs and open MANETs created the urgent need for more sophisticated and

effective solutions. Considerable research has been done and many protocols were devised to provide secure utilization of MANETs.

In recent years, network security has received critical attention from both academia and industry. As the data network becomes more pervasive and its scale becomes larger, network intrusion and attack have become severe threats to network users. This is especially true for the emerging wireless data networks. Compared to their wired counterpart, wireless networks are prone to security attacks ranging from passive eavesdropping to active interfering. As it is even more difficult to protect network entities against the intruders in wireless environment, occasional break-ins in a large-scale mobile network are nearly inevitable over a large time period.

While we may employ sophisticated security techniques into the system design to prevent intrusions, we expect complete intrusion-free systems to be costly and unrealistic, if not impossible at all. Therefore, in order to handle network intrusions, we expect a paradigm shift from completely preventing intrusions to tolerating intrusions to certain extent.

In recent years, infrastructure less ad hoc networking technologies such as MANET and Bluetooth have received critical attention in both academia and industry. This emerging technology seeks to provide users secure service access “anytime” and “anywhere” in a potentially large ad hoc wireless network. The growing commercial and military deployments of these networks have made security design increasingly important.

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without any established infrastructure or centralized authority. Until now, the main research focus has been on improving the protocols for multi-hop routing, performance and scalability of the ad hoc networks. Though, the performance and scalability have their place in wireless network research, the current and future applications of the ad hoc networks has forced the research community to look at dependability and security aspects of ad hoc networks. Security in an ad hoc network is essential even for basic network functions like routing and packet forwarding, since such network functions are carried out by the nodes themselves rather than specialized routers. Hence, the nodes of an ad hoc network must be trusted for the proper execution of basic network functions.

The intruder in the ad hoc network can come from anywhere, along any direction and target any communication channel in the network. Compare this with a wired network where the intruder gains physical access to the wired link or pass through security holes at firewalls and routers. Since the infrastructure-free mobile ad hoc network does not have a clear line of defense, every node must be prepared for the adversary. Hence a centralized or hierarchical network security solution for the existing wired and infrastructure-based cellular wireless networks will not work properly for mobile ad hoc networks.

Securing the ad hoc networks, like any other field of computers, is based on the principle of confidentiality and integrity. These principles exist in every field, but the presence of malicious nodes, covert channels and eavesdroppers in the mobile ad hoc network makes this an extremely important and quite a challenging problem.

MOBILE AD HOC NETWORKS

There are various definitions for the term wireless Mobile Ad Hoc Network (MANET) as in and others. Ad hoc in Latin means "for this purpose only", and it implies spontaneous and temporary setting. Therefore, MANET is a collection of mobile and/or stationary devices connected through wireless links to serve a specific purpose. MANETs provide users with easier ways to connect and communicate without the need for prior setup or a centralized server. Examples of MANET applications are sensor networks (smart dust), military applications, safety/rescue operations, conferences and meetings, and peer-to-peer networks. MANETs are currently used in many areas and have various defining characteristics that differentiate them from other wireless networks such as WLAN. These characteristics are:

- Infrastructure less: MANETs are by nature formed by independent devices wishing to communicate for some purpose and all devices have the same role.

Dynamic Topology : Mobile devices move freely and could be in and out of the network dynamically, constantly changing the links and topology.
Low and Variable Bandwidth'. Wireless links have limited bandwidth than wires. Interference, noise and congestion effects also cause bandwidth to vary with the surrounding conditions. Constrained Resources'. Generally, devices in a MANET are small handheld devices, which have limited power, processing capabilities, and storage.
Limited Device Security: Devices are susceptible to physical problems such as theft, loss and damage. Limited Physical Security. Wireless links are more susceptible to external attacks on the physical layer such as eavesdropping, spoofing, jamming and Denial of Service (DoS).

Because MANETs have a very special setting, they require a different set of security mechanisms. The absence of a centralized authority renders many of the proven security mechanisms impractical (and in many cases, useless). Most of the security mechanisms rely at some stage 011 the existence of a centralized authority to function correctly. New innovative mechanisms need to be devised that will work in the absence of the centralized authority and

the changing topology of the network. Furthermore, MANET nodes are independent, thus do not have the obligation to behave correctly, thus mechanisms to ensure proper
behavior must be considered. Among the different network layers, we view the security of the network layer as an essential aspect to the security of all above layers; therefore, it is important to provide high levels of security at this layer.

RELATED WORKS

There were several proposals of building logical infrastructure for ad hoc networks such as clustering and virtual backbone. To avoid additional overhead and complexity, we do not assume infrastructure support in our design. Communication issues in ad hoc wireless networks are addressed through fully distributed service model and its localized implementation in our architecture.

PGP follows a "web-of-trust" authentication service model. In PGP each entity configures certificates that are learned by out-of-band means. A certificate is accepted if it bears a threshold number of signatures from entities that are already known to be trustworthy. However, this approach does not scale beyond a relatively small community of trusted individuals. In a mobile system, any two entities will potentially meet, communicate with, and route packets for each other. It would be difficult for each entity to maintain a long list of trusted friends, potentially as large as the list that contains all nodes in the whole network. We address the scalability issue through a localized trust model where a locally trusted entity that is identified by a fixed-length certificate is globally accepted.

Security function sharing has been a very active research area in the literature. where threshold secret sharing serves as a basic primitives. Resilience against compromised nodes is enhanced by distributing the functionality of the centralized CA servers among a fixed group of servers.

Proactive secret sharing can further improve robustness via periodic secret share updates. However, the focus of these works is to maximize the security of the shared secret in the presence of possible compromises of the secret shareholders. They typically assume a small group of a few servers with rich connectivity. Our scheme is motivated by these works, but extends the idea further in an attempt to minimize the effort and complexity for mobile clients to locate and contact the service providers. We devise scalable algorithms and protocols to enable the distribution of the certification services into every node. There is no differentiation of servers and clients in our architecture any more: a threshold number of any nodes can collaboratively act as servers to provide services for other nodes. Besides, our solution typically works within one-hop neighborhood and does not involve multihop wireless communication.

PROBLEMS AND SECURITY IN MANET

Mobile ad-hoc networks have properties that increase their vulnerability to attacks. Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application-specific trade-offs between security and resource consumption of the device. Mobility/Dynamics make it hard to detect behavior anomalies such as advertising bogus routes, because routes in this environment change frequently. Self-organization is a key property of ad-hoc networks. They cannot rely on central authorities and infrastructures, e.g. for key management. Latency is inherently increased in wireless multi-hop networks, rendering message exchange for security more expensive. Multiple paths are likely to be available. This property offers an advantage over infrastructure-based local area networks that can be exploited by diversity coding.

Besides authentication, confidentiality, integrity, availability, access control, and nonrepudiation being harder to enforce because of the properties of mobile ad-hoc networks, there are also additional requirements such as location confidentiality, cooperation fairness and the absence of traffic diversion.

The lack of infrastructure and of an organizational environment of mobile ad-hoc networks offers special opportunities to attackers. Without proper security, it is possible to gain various advantages by malicious behavior: better service than cooperating nodes, monetary benefits by exploiting incentive measures or trading confidential information; saving power by selfish behavior; preventing someone else from getting proper service, extracting data to get confidential information, and so on.

Routes should be advertised and set up adhering to the routing protocol chosen and should truthfully reflect the knowledge of the topology of the network. By diverting the traffic towards or away from a node, incorrect forwarding, no forwarding at all, or other non-cooperative behavior, nodes can attack the network. Several routing and forwarding attacks have been described.

PROTECTED ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORK

Routing protocols are studied extensively for MANETs and many well-designed protocols are available. Many of these protocols are proven to provide adequate security against most attacks

provided that they have that initial authentication. Here we will first discuss the different types of MANETs based on their context and applications. The three categories dictate how successful the routing protocols are and what requirements need to be fulfilled.

- Organized'. MANETs, with well-defined purpose such as military networks in a battle field and disaster relief operations, where ad hoc networks are formed between members of the teams to serve a well-defined purpose, hi this situation, initial authentication is not a problem since all members belong to the same organization and share the same goals. Therefore, there is no reason for nodes to misbehave or disrupt the network. However, this type of network requires strong authorization and confidentiality measures to secure it against external attacks and compromised devices, hi addition, it may be essential to conceal the locations of these nodes during operation.

- Localized: MANETs, semi-static ad hoc networks that are formed by devices in close proximity of each other such that they can all authenticate each other by physical contact. This type of network is also
referred to as spontaneous networks, hi this case, initial authentication is not a problem. Nevertheless, these networks require authorization and access control mechanisms to ensure that members have access only to resources they are allowed to use.

EVALUATION OF IMPLEMENTATION

We implemented our design in both Unix platforms and a popular network simulator ns-2. Our Unix implementation seeks to quantitatively characterize the computational cost of our solution, and we use the simulation experiments to evaluate communication aspects, such mobility, ubiquitous service availability and channel dynamics in wireless ad hoc networks.

Implementation Issues : The design of our protocols and algorithms is flexible to allow implementation at any layer above the MAC layer in the networking protocol stack. Moreover, it does not make specific assumptions on the network and transport layer protocols. We choose an application-layer implementation for several reasons: (a) We avoid modifications of lower-layer protocols such as packet and frame formats. This facilitates incremental deployment. (b) We achieve maximal independency of the underlying network configurations. This improves the portability and extensibility. (c) We can evaluate the communication efficiency of our security protocols without any specific performance enhancements provided by lower layers.

Evaluation on Communication Aspects : We implemented all the communication protocols at the application-layer in the network simulator ns-2. We developed a UDP-like transport agent that allows for delivery of actual application data units (ADUs) and one-hop broadcast.

CONCLUSION

In this paper we have considered the security aspects concerning a mobile ad hoc network. Our analysis shows that the potential threats faced by MANETs come in the form of denial of service, selfish node behavior, or routing attack. The taxonomy developed hi this paper
highlights the contributions by various authors and shows the different types of approaches taken to provide security. This taxonomy should help researchers focus on specialized methods needed to secure MANETs.

In this paper, we have described a solution to security support in wireless mobile networks. Our design has been motivated by three main factors: (a) We do not believe that any security system is completely unbreakable. Therefore, our design has to work in the presence of such break-ins. (b) We seek to maximize the service availability in each network locality; this is crucial to supporting ubiquitous services for mobile users. (c) The solution has to be fully decentralized to operate in a large-scale network. To this end, we have addressed networking issues including mobility, scalability, service ubiquity, and network dynamics such as channel interference and node failures. Our experiences in implementation and simulations have shown positive results for our approach.

REFERENCES

1. Buttyan L. and Hubaux J. P., "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks." ACM Journal for Mobile Networks (MONET), Special issue oil Mobile Ad Hoc Networks. 2002.

2. Fox and S. D. Gribble. Security on the Move: Indirect Authentication using Kerberos. In MOBICOM, pages 155–164, 1996.

3. Frank Stajano and Ross Anderson. The Resurrecting Duckling. Lecture Notes in Computer Science, Springer-Verlag, 1999.

4. Haiyun Luo, Songwu Lu Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks, Technical Report TR-200030, Dept. of Computer Science, UCLA, 2000.

5. J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc

Network Routing Protocols. In MOBICOM, pages 85–97, 1998.

6. J. Hastad, J. Jonsson, A. Juels, and M. Yung. Funkspiel Schemes: an Alternative to Conventional Tamper Resistance. In ACM CCS, 2000.

7. Kong J.. Zerfos P.. Luo H.. Lu S., and Zhang L., "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," in Proceedings of IEEE International Conference on Network Protocols, Riverside, CA. November 2001.

8. Levente Butty´an and Jean-Pierre Hubaux. Enforcing Service Availability in Mobile Ad-HocWANs. In Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (Mobi- HOC), Boston, MA, USA, August 2000.

9. Michiardi P. and Molva R.. "Prevention of Denial of Service Attacks and Selfishness in Mobile Ad Hoc Networks," Research Report, 110. RR-02-063, histitut Eurecoin, Sophia-Antipolis, France, January 2002.

10. Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In Proceedings of MOBICOM 2000, pages 255–265, 2000.