ISSN 2319-2720

Volume 2, No.3, July - September 2013

International Journal of Computing, Communications and Networking

Available Online at http://warse.org/pdfs/2013/ijccn02232013.pdf

Survey of Secure Communication Techniques in Mobile Ad-hoc Network

Deepak Chopra[1] **Shaila Chugh**[2] **Deepak Sain**[3]

[1]M.Tech Scholar, Dept. of IT, SATI, Vidisha (M.P.), *deepakchopra.rgtu@gmail.com*

[2]Dept. of IT, SATI, Vidisha (M.P.), *Shailachugh@gmail.com*

[3]Dept. of IT, SATI, Vidisha (M.P.), *dsain30@yahoo.in*

Abstract

A Mobile ad hoc Network is an autonomous network comprised of free roaming nodes which communicate wireless by radio transmission. One of the main challenges in MANETs is the design of efficient and light-weight security algorithms that can be handled by devices with limited computational capabilities. Efficiency, reliability and security are (competing) design goals for algorithms suitable for MANETs.

Many protocols neglect at least one of these goals: While cryptographic algorithms are typically provable secure and reliable to the extent that lost messages are simply handled with retrials, they marginally consider communication costs. Many state of the art algorithms have a computational and communicational complexity that exceeds the capabilities of resource-constrained MANETs. To overcome these efficiency barriers, new protocols need to be developed that exploit the specific infrastructure as provided by the MANET.

In this paper we represent a survey of secure communication techniques in Mobile Ad-hoc Network. The data mining techniques are categorized based upon different approaches like key management, Authentication, secure routing techniques.. This paper provides the major advancement in the secure MANET based secure communication research using these approaches the features and categories in the surveyed work.

Keywords - MANET, Secure Routing, Key management, Performance Analysis.

1. *INTRODUCTION*

Mobile Ad-hoc Network (MANET) is often characterized by rapidly changing and unpredictable wireless topology. Because the multiple nodes in such a system can enter and leave the system at any time, this system requires some sensing of the location and hence offers a very attractive environment to support context aware applications. The mobile ad-hoc network provides limited automation needed in the position calculation and is an ideal and cheap alternative in the environment where the infrastructure is not developed yet. Bluetooth is one such emerging technology that provides ad-hoc networking [1-3].

The major challenges to mobile ad hoc networks concern their design and operation, and result mainly from the lack of a centralized entity and infrastructural elements such as base stations, communication towers and access points. The possibility exists of fast node movement and all communications are conducted through a wireless medium. These unique characteristics present nontrivial challenges for mobile ad hoc networks.

As previously stated, many applications have recently become dependent on mobile ad-hoc networks, and security is an extremely serious issue in any network. The dynamic nature of mobile ad-hoc networks makes it extremely challenging to ensure secure transmission in these networks, which rely on the collaboration of all their nodes for their creation and efficient operation. While maintaining suitable routing information in a distributed way is a challenging issue in such networks, it is even more challenging to secure the protocols used for routing. At the network level, mobile *ad hoc* system fundamentally requires the routing protocols to be secured, as they enable a communication path to be established.

On the other hand, the design of most such routing protocols gives no consideration to security, working instead with an implicit assumption of trust among the nodes. This provides the opportunity for malicious attackers, who may intend to bring down the network. In this paper we discussed a survey of secure communication techniques in Mobile Ad-hoc Network [2-4].

2. *BACKGROUND TECHNIQUES*

Secure Routing in Mobile *Adhoc* Networks

The nodes in mobile *ad hoc* wireless networks act both as regular terminals (source or destination) and as routers for other nodes in the network, unlike fixed wired networks such as the Internet, where dedicated routers are controlled by a service provider. This absence of dedicated routers makes the provision of security a challenging task in *ad hoc* wireless networks, where the task of ensuring secure communication is also made difficult by factors including the mobility of nodes, limited processing power and limited availability of resources such as battery power and bandwidth. The requirements of a secure routing protocol for mobile *ad hoc* wireless networks are as follows:

→***Detection of malicious nodes:*** If there are malicious nodes in a network, then a secure routing protocol should be able to detect them and avoid selecting them in the routing process.

→***Guarantee of correct route discovery:*** The protocol should be able to find a route when one exists between the source and the destination; it should also ensure that it is correct.

→***Confidentiality of network topology:*** Malicious nodes will be able to view disclosure and information regarding network topology that may lead to an attack on these networks. The confidentiality of the network topology is an important requirement in order to prevent a potential attacker from studying the traffic pattern of the network. Thus, the attacker will not be able to discover the active nodes in *ad hoc* wireless networks and all attempts to mount e.g. Denied of Service (DoS) attacks against such bottleneck nodes will fail.

→***Stability against attacks:*** The routing process in mobile *ad hoc* wireless networks should not be disrupted permanently by passive or active attackers. The routing protocol must be self-sustainable; thus it must be able to revert to its normal operating state within a finite amount of time after a passive or active attack. The protocol must ensure Byzantine robustness; that is, the protocol should work correctly even if some of the nodes which have previously participated in the routing process turn out later to be malicious or are intentionally damaged [1] and [3] and [5].

Proactive RSA

The proactive RSA protocol was not designed in particular for mobile *ad hoc* networks; however, many other protocols used in this type of network are based upon it. The essential characteristic of the proactive RSA is that it uses distributed shared keys. It is more difficult for an adversary to find these, because they are updated frequently. The device is a mechanism used to share a key and update it frequently without revealing secret values; these are the main goals of this protocol, which functions by communicating through an authenticated bulletin board. The avoidance of jamming and the capability of nodes to restart (re-initialize) a compromised node are the main advantages of this protocol. On the other hand, it supplies only probabilistic stages of security and requires a trusted dealer to authenticate the initial group to create the authenticated bulletin board.

Security-aware A*d Hoc* Routing Protocol

The Security-aware mobile a*d hoc* Routing (SAR) protocol uses security as one of the key metrics to find paths, incorporating a structure for enforcing and measuring features of the security metric. This structure uses different levels of security for different applications that use the SAR protocol for routing. The communications between end nodes in *ad hoc* wireless networks are made through (possibly multiple) intermediate nodes, depending on the fact that the two end nodes trust the intermediate nodes. One of the tasks of SAR is to define the level of trust as a metric for routing.

This means that every path for packets is associated with a security level, which is determined by a numerical calculation. A certain level of security is also associated with every intermediate node. When an intermediate node receives a packet it compares its level of security with that defined for the packet, and if the packet‘s security level is less than that of the node, then this node is considered to be a secure node and is permitted to view the packet. If it is greater, the packet is simply discarded. The SAR mechanism could easily be incorporated into traditional routing protocols for *ad hoc* networks. SAR permits the application to select the level of security it requires; however, the protocol requires different keys for different levels of security. The main disadvantage of this mechanism is that it tends to increase the number of keys required when the number of security levels used increases [2] and [6].

Authenticated Routing Protocol

The Authenticated Routing *Ad hoc* Network (ARAN) protocol provides secure routing for *ad hoc* wireless networks by means of cryptographic certificates that successfully defeat all identified attacks in the network layer. It takes care of authentication, message integrity and non-repudiation, but expects a small amount of prior security coordination among nodes. In general, the main requirements it attempts to fulfill are first preventing things such as the spoofing of routing signals, the fabrication of routing packets, the shaping by adversaries of routing loops and the exposure by routing packets of the network topology;

and secondly ensuring that such routing packets are not altered during transmission and that the shortest routing path is utilized.

The major drawback of the protocol is that it needs a trusted certification server to issue the initial certificates. It offers security at two levels. The first, which is not fully secure, is an end-to-end authentication that is effective and requires low CPU power; however, it does not guarantee the shortest path usage. The second is stronger in security and guarantees to provide the shortest path, but requires more CPU power and resources [6-8].

3. SURVEY OF SECURE COMMUNICATION TECHNIQUES IN MANET

3.1 Encryption Methodology for Secure Communication in MANET

Ditipriya Sinha and Uma Bhattacharya and Rituparna Chaki et. al. proposed a secure encryption strategy using Chinese Remainder Theorem for shielding data from unauthorized access. The paper also includes a comparison of proposed method with existing methods. MANETs are well known for their flexibility and ease of communication. The communication is purely based on trust, without any need of authentication. This often leads to insecure communication, causing information tampering. The traditional means of security are not sufficient to safeguard against the inherent dangers of MANET.

Researchers around the world are working in this issue. The preferred mode of securing data is through encryption. The process of encryption however is complex enough to increase the computational overhead. This paper proposes a new security scheme in MANETs. This paper uses combination of RSA and CRT schemes for key generation, encryption and decryption of data. In this paper encryption is done using RSA scheme. On the other hand encrypted data is decrypted with the help of CRT scheme. Computational complexity of CRT is less than RSA modular exponentiation scheme. For this reason CRT scheme is used in this proposed scheme. Detection of secure routes is another goal of this proposed work. For secure route detection this paper creates safety key.

This safety key is divided into n pieces in such a way that safety key is easily reconstruct from any k pieces. These pieces are shared among n different routes to detect whether the routes are secure or not. Secure paths are detected with the help of Shamir’s secret sharing using Lagrange’s Interpolation scheme. This algorithm combines the concepts of RSA, CRT and Shamir’s secret sharing. These combinations provide secure environment in MANETs. This involves routing of packets in a confidential manner. Much work has been done in this area, most of the researchers have considered RSA algorithm for key encryption. The use of RSA has however increased the overload on the network. This paper proposes the use of Chinese Remainder theorem along with Shamir’s secret sharing to reduce the encryption complexities. Secure path detection, encrypted message transformation are main objective of this protocol.

The proposed protocol not only generates key for encryption and decryption but also generates secure routes for transmitting messages in encrypted form.
The proposed protocol will need to improve in secure routing for better overall performance in future [1].

3.2 Secure Multicast Communication for MANET

D.Suganya Devi and Dr. G.Padmavathi et. al. , in which source node uses Multicast version of Destination Sequenced Distance Vector(MDSDV) routing protocol to collects its 1 hop neighbors to form cluster and each node which have child node is elected as the Local controllers of the created clusters. It also tolerates the faults that causes due to failure of nodes. This paper proposed an efficient cluster-based multicast tree (CBMT) algorithm for secure multicast communication for mobile adhoc networks. Thus this new efficient CBMT approach is a dynamic clustering scheme with mobility aware Multicast version of DSDV routing protocol, which becomes easy to elect the local controllers of the clusters and updates periodically as the node joins and leaves the cluster. It tolerates the fault that causes due to node failure.

The main objective of the paper is to present an efficient approach for secure multicast communication for mobile ad-hoc network by overcoming issues of average end to end delay due to node failure and tolerates the fault that occurs during multicast communication. Secure multicast communication is a significant requirement in emerging applications in ad-hoc environments like military or public emergency network applications. Membership dynamism is a major challenge in providing complete security in such networks. Some of the existing algorithms like OMCT address the critical problems using clustering approach like 1-affects-n phenomenon and delay issues.

Therefore an attempt is made to reduce the end to end delay and improve the fault tolerance as node increases by using an approach of efficient Cluster Based Multicast Tree algorithm for fault tolerant multicast communication. This algorithm uses Mobility aware Multicast version of DSDV routing protocol for electing LCs. The proposed efficient CBMT is tested and the entire experiments are conducted in a simulation environment.

The proposed method is efficient and more suitable for secure multicast communication dedicated to operate in MANETs. The proposed method is not more efficient in large number of node operate in MANETs [2].

3.3 Security Scheme for Data Integrity in MANET

A. Rajaram and Dr. S. Palaniswami et. al. proposed scheme makes use of Shamir's secret sharing scheme along with a redundancy technique to support certificate renewal and revocation. The malicious nodes are detected by the trusting mechanism by monitoring the behavior hop by hop. By simulation results, we show that the proposed scheme achieves more packet delivery ratio while attaining less delay and overhead, compared with the previous existing scheme.

They proposed a hop-by-hop authentication protocol. It authenticates packets at every hop by using a certificate authority (CA) based approach and drops any packets that originate from outsiders. Each node monitors and evaluates the behavior of its successors by itself, and as soon as it accuses a node it launches a procedure to approve this accusation. In previous work, they had analyzed about the confidentiality and authentication of data in MANET environment.

In this paper, they analyzed the integrity of data along with the external attack.
The scheme was contributed with three components;
→ Monitoring Routing cum forwarding (RCF) behavior
→ Certificate Revival.
→ Certificate Revocation.
Monitoring Routing cum forwarding (RCF) behavior which is based on our previous work, involves detecting misbehaviors in both the routing as well as the packet forwarding in the network. Certificate revival uses a redundancy scheme in which a node is allocated more than one key share by incorporating redundancy into the network. This mechanism guarantees that genuine nodes can continue to stay in the network by revival of their certificates along a periodical time period. Certificate revocation provides the authority to isolate any malicious nodes or regain the nodes which turn up to its best state after any attack or failure. Thus, Certificate revival and Certificate revocation added to our previous work brings forth the integrity factor along with confidentiality and authentication.

They used Shamir's secret sharing model with redundancy for Certification revival and revocation. When used redundancy the challenges of node mobility reduces as it states that the total number of nodes requisite to recreate the CA key can be less than $(k - 1)$. This increases the integrity of the network and provides the network nodes to be more mobile. Certification revocation is done using the trust values of the nodes.

The proposed scheme achieves more packet delivery ratio while attaining less delay and overhead.
The proposed scheme will need to improve in certificate authentication for better security [3].

3.4 Secure Routing Protocol Based on Ad Hoc Network

Li-Li PAN et. al. forwarded a secure Ad Hoc On Demand Routing (SAHODSR) protocol which adapts for Ad hoc network aiming at the mobile ad hoc network(MANET) routing protocol attacks and typical routing scheme of security problems. This protocol uses serial number of destination node, list session keys of neighbor nodes between the mobile nodes and message authentication code(HMAC) based on hash function to verify the validity of routing discovery and route reply. Neighbor nodes defend against a variety of attacks through binding MAC address with it's ID. Its best performance is self-certified key system and generate new share key with non-interactive manner which brings to very little communication cost and improve the efficiency in executing.

Routing attacks can mainly be divided into passive attacks and active attacks. Passive attacks do not destroy the normal operation of routing protocol. They only listen to the network routing information, from which to obtain useful content. Active attack means that malicious nodes prevent the establishment of routings, change the direction of packet transmission, interrupt the use of routings and use false data to obtain network authentication and authorization etc.

Active attacks are divided into routing destroy attacks and resource consumption attacks. After the security analysis as well as the Ns-2 simulation, we can find that SAHODSR protocol can defends and resist a variety of attacks, such as denial of service attacks, forgery attacks on the source node and destination node, tampering attacks, black hole attacks, wormhole attacks, etc. The proposed scheme achieved better safety performance through the costs of paying more route discovery time than the DSR. The proposed scheme needs to reduce the end to end delay [4].

3.4 QoS of Dynamic Authentication Bandwidth Management for the Wireless Environment

Amanda Peart, Mo Adda et. al. proposed a dynamic wireless bandwidth management system that allocates bandwidth dynamically to users as they authenticate with a wireless access point (AP). As users log into the system and out on an adhoc basis the bandwidth is dynamically redistributed with each event. This paper introduced a wireless bandwidth management system that allocates bandwidth dynamically to users as they authenticate with wireless access points (AP).

Furthermore the implementation test results illustrate how the bandwidth dynamically changes when new users are accepted and authenticated to access the bandwidth. This report discusses current solutions for managing central, authentication based wireless access to networks, specifically for networks where public users are granted access and the level of trust cannot be guaranteed. This paper also discusses why network access for these users needs to be controlled in order to mitigate abuse. Additionally current solutions used to limit user's bandwidth by utilizing RADIUS attributes stored in a database, analysing the flaws within these proposed solutions the most prominent being that of the techniques used for bandwidth allocation.

Additionally bandwidth allocation was static even if there were a limited number of users using an AP they would only be permitted a specific amount. This would effectively waste bandwidth, which could potentially be given to users making use of these AP's. This proposed solution dynamically allocates bandwidth based on the number of users utilizing the AP.

Future work can be made on grouping specific users into priority groups where they would be permitted more bandwidth, and then the remaining bandwidth would then be divided amongst the less priority users [5].

3.6 Multipath Routing Protocol inAd-Hoc Networks for Improving Security:

Cuirong Wang, Shuxin Cai and Rui Li et. al. proposed a secure routing protocol based on multipath routing technology, namely AODVsec, which divides a data unit into several data pieces and transmits these pieces through different paths. By setting security level on each node, AODVsec limits the maximum number of data pieces an intermediate node can forward. In this way, the malicious node cannot get enough data information for breaking the encryption algorithm. Route maintenance is done using route error (RERR) packets.

When a link failure is detected (by a link layer feedback, for example), a RERR is sent back via separately maintained predecessor links to all sources using that failed link. Routes are erased by the RERR along its way. When a traffic source receives a RERR, it initiates a new route discovery if the route is still needed. Unused routes in the routing table are expired using a timer-based technique. AODV limits the generated path number by controlling broadcast list. As a node receives RREQ from source at the first time, a new reverse path is added to local broadcast list. As the node receives another RREQ from source, it looks up in the local broadcast list. Once the RREQ form that source is existed, the new received RREQ is dropped. Therefore, the traditional AODV can only generate a single path.

In this paper, based on multipath routing technology, they proposed a multipath routing protocol for improving security, AODVsec. Followed by introduction of AODVsec's implementation, they evaluated AODVsec under ns2 simulation environment with comparison of traditional multipath routing protocol. The results show that AODVsec outperforms traditional multipath routing on ensuring security. As a common case, attacker can not intercept all the paths; AODVsec avoids maliciously accessing a entire data packet, so it improves system's security with negligible routing overhead. As a future work, it will focus on designing the synchronization control mechanism to solve this problem [6].

After surveying different techniques we define the Merits and Demerits of techniques in the table:

Techniques	Merits	Demerits
MANET, Chinese Remainder Theorem, Safety Key, Super Key	The proposed protocol not only generates key for encryption and decryption but also generates secure routes for transmitting messages in encrypted form.	The proposed protocol will need to improve in secure routing for better overall performance in future [1].
Cluster based multicast tree, MDSDV, Mobile Adhoc Networks, Secure Multicast Communication.	The proposed method is efficient and more suitable for secure multicast communication dedicated to operate in MANETs.	The proposed method is not more efficient in large number of node operate in MANETs [2].
MANET, Denial of Service (DoS), Routing cum forwarding (RCF), Certificate revocation, Certification revival.	The proposed scheme achieves more packet delivery ratio while attaining less delay and overhead.	The proposed scheme will need to improve in certificate authentication for more security [3].
MANET; on-demand source routing protocol; secure routing;	The proposed scheme achieved better safety performance through the costs of paying more route discovery time than the DSR.	The proposed scheme needs to reduce the end to end delay [4].
Quality of Service; bandwidth management; wireless networks;	This proposed solution dynamically allocates bandwidth based on the number of users utilizing the AP.	Future work can be made on grouping specific users into priority groups where they would be permitted more bandwidth, and then the remaining bandwidth would then be divided amongst the less priority users [5].
Aad-hoc networks, Multi Path Routing AODV, trust level.	AODVsec avoids maliciously accessing a entire data packet, so it improves system’s security with negligible routing overhead.	Proposed Scheme focused on designing the synchronization control mechanism to solve this problem [6].

4. CONCLUSION

MANETs have the potential to be applicable to a large range of applications that are currently conducted in more traditional networks. In many emergency cases, these applications can provide more comprehensive and reliable information, thus helping to minimize risks. However, communication over a wireless channel opens many possibilities for interception and manipulation. Therefore, the protocols used in military MANETs need to be secure against a wide range of attacks.

To provide robustness against compromised nodes, the investigation possibilities to distribute the power for performing security critical computations in a MANET. While protocols for specific techniques and applications were introduced in this survey, the development of communication of secure routing protocols for a wide range of applications for MANETs is a major task for our future research.

REFERENCES

[1] Ditipriya Sinha and Uma Bhattacharya and Rituparna Chaki, " **A CRT based Encryption Methodology for Secure Communication in MANET**", International Journal of Computer Applications (0975 – 8887) Volume 39– No.16, February 2012, pp. 20-25.

[2] D.Suganya Devi and Dr. G.Padmavathi, "**Efficient Cluster Based Multicast Tree for Secure Multicast Communication for Mobile Ad Hoc Networks**", International Journal of Engineering Science and Technology Vol. 2(5), 2010, pp.1304-1310.

[3] A.Rajaram and and Dr.S.Palaniswami, "**The Modified Security Scheme for Data Integrity in MANET**", International Journal of Engineering Science and Technology Vol. 2(7), 2010, pp. 3111-3119.

[4] Li-Li PAN, "**Research and Simulation for Secure Routing Protocol Based on Ad Hoc Network**", 2nd International Conforence on Education Technology and Computer (ICETC), V5, pp. 46-49, 2010.

[5] Amanda Peart, Mo Adda, "**Quality of Service: Dynamic Authentication Bandwidth Management for the Wireless Environment**", 1st International Conference on Information Science and Engineering (ICISE2009), pp.- 5366-5369,2009.

[6] Cuirong Wang, Shuxin Cai and Rui Li, "**AODVsec: A Multipath Routing Protocol in Ad-Hoc Networks for Improving Security**", International Conference on Multimedia Information Networking and Security, pp. 401-404, 2009.

[7] S.Sarkar,B.Kisku,S.Misra and M.S Obaidat, "**Chinese Remainder Theorem-Based RSA-Threshold Cryptography in MANET using Verifiable Secret Sharing Scheme**" IEEE International Conference On Wireless and Mobile Computing,Networking and Communications,2009.

[8] A.Amuthan and B.Arvind Baradwaj, "**Secure Routing Scheme in MANETs using Secret Key Sharing**", International Journal of Computer Applications (00975-8887) volume 22-No.1, May 2011.