ISSN:0975-9646

Review of Neighbor Coverage Based Probabilistic Rebroadcast with Cryptographic Technique

Nishakumari Ashokkumar Lodha
Assistant Professor
Department of Computer Science
G.H.R.I.E.M, Jalgaon

Dipali Sakharam Patil
M.E.(C.S.E) Student
Department of Computer Science
G.H.R.I.E.M,Jalgaon

***Abstract*—Mobile Ad Hoc Network (MANETs) consists of a collection of mobile nodes which can move freely. These nodes have characteristic that they can be dynamically self-organized into arbitrary topology networks without a fixed infrastructure. MANETs are highly dynamic network because nodes may join and leave the network at any time. NCPR significantly reduce the routing overhead in the MANET. Once the route is selected from source to destination data is transferred between nodes. This transmission is unsecured. To make it secure a cryptographic technique can be applied.**

***Index Terms*—MANET routing, communication phases, NCPR, paillier cryptosystem**

I. Introduction

A MANET is a network that consists of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. The mobile hosts do not have any centralized control like base stations or mobile switching centers. This offers unrestricted mobility and connectivity to the users, although the duty of network management is now entirely on the nodes that forms the network. Due to the limited transmission range of wireless network interfaces, multiple hops may be needed for one node to exchange data with another across the network.

The routing protocols for MANET are classified as table driven i.e. proactive routing protocol, on demand i.e. reactive routing protocol and hybrid routing protocol. In proactive routing, nodes attempt to maintain consistent, up-to-date routing information of the whole network. Each node has to maintain one or more tables to store routing information, and response to changes in network topology by broadcasting and propagating. Reactive routing tries to eliminate the conventional routing tables and consequently reduce the need for updating these tables to track changes in the network topology. When a source requires to a destination, it has to establish a route by route discovery procedure, maintain it by some form of route maintenance procedure until either the route is no longer desired or it becomes inaccessible, and finally tear down it by route deletion procedure. Hybrid routing protocols aggregates a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used. Consequently, in hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones [4].

Due to high mobility of nodes in network there is frequent path failure and route discovery in MANET. So the NCPR (Neighbor coverage based probabilistic rebroadcast) is used for reducing this routing overhead in Mobile Ad Hoc Networks. In this routing protocol the neighbor knowledge and rebroadcast probability is used for rebroadcasting a request. A novel rebroadcast delay is calculated to determine the rebroadcast order while routing, and it obtains the more accurate additional coverage ratio by sensing neighbor coverage knowledge. A connectivity factor is defined to provide the node density adaptation for keeping the network connectivity. By combining the additional coverage ratio and connectivity factor, the rebroadcast probability is calculated. [1].

The communication in mobile ad hoc networks comprises two phases,

1. Route discovery and
2. Data transmission.

In an adverse environment, both phases are vulnerable to a variety of attacks. The adversaries at data route discovery phase can disrupt the route discovery by impersonating the destination, by responding with stale or corrupted routing information, or by disseminating forged control traffic. This way, attackers can obstruct the propagation of legitimate route control traffic and adversely influence the topological knowledge of benign nodes. However, adversaries can also disrupt the data transmission phase and, thus, incur significant data loss by tampering with, fraudulently redirecting, or even dropping data traffic or injecting forged data packets.

To provide comprehensive security, both phases of MANET communication must be safeguarded. It is notable that secure routing protocols, which ensure the correctness of the discovered topology information, cannot by themselves ensure the secure and undisrupted delivery of transmitted data. This is so, since adversaries could abide with the route discovery and be placed on utilized routes. But then, they could tamper with the in-transit data in an arbitrary manner and degrade the network operation [4].

The requirements of Secure Communication in MANET are

(a) It is necessary that a security association exist between network members to ensure authentication and non-repudiation for trusted nodes.

(b) Sensitive information must be exchanged confidentially.
(c) Integrity of the information exchanged within the network has to be maintained [4].

There are numerous security routing protocols and key management schemes that have been designed based on cryptographic techniques. These techniques include public key infrastructures and identity-based cryptography. In fact, some of them are fully adapted to fit the network requirements on limited resources such as storage, CPU, and power limitations[9]. The Paillier Cryptosystem is a modular, public key encryption scheme, created by Pascal Paillier, with several interesting properties[7].

This paper covers the literature review of routing protocol and different techniques used for secure communication in MANET in section II. Section III contains the overview of NCPR protocol and section IV contains the paillier cryptographic method. The section V concludes the paper.

II. Literature Review

In [2] AdhocOn Demand Distance Vector Routing AODV is a novel algorithm for the routing operation of such mobile adhoc networks. AODV is an on demand routing protocol i.e. the routes are obtained as needed. The route request packet (RREQ) is sent from source to destinationand the route is returned in route reply packet (RREPL) from destination to source. In [1] the neighbor coverage based probabilistic rebroadcast protocol (NCPR) has proposed that utilizes the AODV mechanism. NCPR reduces routing overhead as part of rebroadcast.

In [4] have discussed several main requirements that need to be achieved to ensure the security of the mobile ad hoc network to find out how to judge if a mobile ad hoc network is secure or not. The security criteria include availability, Integrity, Confidentiality, authenticity, nonrepudiation, authorization, anonymity. There are some types of attacks in mobile ad hoc network. The attacks in MANET can be briefly classified into two categories: external attacks and internal attacks the main attack types in the mobile ad hoc network, which are denial-of-service (DoS) attacks, impersonation attacks, eavesdropping attacks and attacks against routing. Two kinds of popular security techniques in the mobile ad hoc network, which are intrusion detection techniques and secure routing techniques.

To provide comprehensive security, both phases of MANET communication must be safeguarded. To secure the data transmission phase, [3] propose and evaluate the Secure Message Transmission (SMT) protocol, an end-to-end secure data forwarding protocol tailored to the MANET communication requirements. The SMT protocol safeguards pairwise communication across an unknown frequently changing network, possibly in the presence of adversaries that may exhibit arbitrary behavior.

In [9] has explained the scenario for using symmetric and asymmetric cryptosystem in a MANET network.If all routing messages are encrypted with a symmetric cryptosystem, it means that everybody those want to be able to participate in the network has to know the key. If there is a team of persons, let every member of the team to know the “team-key”. They assume that a member of the team will not do anything nasty to the other members because the members of team trust each other. They trust and authorize the other members to change their routing tables. Suppose that a MANET network need to be created where everybody can participate. May be in a convention, in a meeting room, in a campus, or in our neighborhood.At that time there is problem, they do not trust others. With this scenario in mind, the best option could be to use an asymmetric cryptosystem (with public and private key pairs) so that the originator of the route messages signs the message. It would not be needed to encrypt the routing messages because they are not secret. The only requirement is that the nodes will be able to detect forged routing messages.

In [5] a new routing technique called security aware ad hoc routing that incorporates security attributes as parameters in to ad hoc route discovery. SAR enables the use of security as a negotiable metric to improve the relevance of route discovered by ad hoc routing protocols. A two tier classification of routing protocol security metrics, and propose a framework to measure and enforce security attributes on ad hoc routing paths. In addition to determining a secure route, the information in routing messages must also be protected against alteration that can change routing behavior. The security of ad hoc routing algorithm is improved with respect to transmission of routing messages. Zapata and Asokan in [6] proposed SAODV i.e. a Secure version of AODV which uses digital signature and hash chains to secure the routing messages.

In [7] the security of routing protocols for ad hoc network has been discussed. In an ad hoc network, from the point of view of a routing protocol, there are two kinds of messages: the routing messages and the data messages. Both have a different nature and different security needs. Data messages are point-to point and can be protected with any point-to-point security system (like IP Sec). On the other hand, routing messages are sent to immediate neighbors, processed, possibly modified, and resent. Moreover, as a result of the processing of the routing message, a node might modify its routing table. This creates the need for the intermediate nodes to be able to authenticate the information contained in the routing messages (a need that does not exist in point-to-point communications) to be able to apply their import authorization policy.

By using unique characteristic of Mobile Ad hoc network most applications were developed. The security issue of routing information was an issue not addressed in recent routing protocol. Several potential problems are presented in [14] including computational overload attack, node compromise, energy consumption, and black hole attack. In [15] attacks are categorized as manipulation of routing information and exhaustive power consumption and provide detailed treatment of many characteristic attacks.

III. Overview Of Ncpr Protocol

Neighbor Coverage based probabilistic rebroadcast is a novel scheme that calculates the

rebroadcast delay.Rebroadcast delay is used to determine the forwarding order**.** The node which has more common neighbors with the previous node has the lower delay. If this node rebroadcasts a packet, then more common neighbors will know this fact. Therefore, this rebroadcast delay enables the information that the nodes have transmitted the packet spread to more neighbors. The protocol also calculates the rebroadcast probability that considers the information about the uncovered neighbors (UCN), connectivity metric and local node density to calculate the rebroadcast probability. The rebroadcast probability is composed of two parts[1]:

- Additional coverage ratio, which is the ratio of the number of nodes that should be covered by a single broadcast to the total number of neighbors, and
- Connectivity factor, which reflects the relationship of network connectivity and the number of neighbors of a given node.

IV. PAILLIER CRYPTOSYSTEM

This section shows how to encrypt and decrypt messages using pailliercryptosystem, with the underlying mathematical principles that make the system work clearly outlined. It is assumed that the reader is familiar, to some degree, with modular arithmetic, as well as the concept of converting an alphanumeric message into a purely numeric message, which can be broken into blocks, m_i, such that, for each i, $0 < m_i < n$, for a predetermined value, n. Also, the term plaintext will be used to refer to a message that is numeric, but is not encrypted, while the term cipher text will be used to refer to plaintexts which have been encrypted, but not yet decrypted [7].

Using Paillier Cryptosystem

1. Select two large prime numbers p and q randomly and independently of each other such that $gcd\big(pq, (p-1)(q-1)\big) = 1$ This property is assured if both primes are of equal length
2. Compute $n = pq$ and $\lambda = lcm(p-1, q-1)$
3. Select random integer g where $g \epsilon\, \mathbb{Z}^*_{n^2}$
4. Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse $\mu = \left(L\left(g^{\lambda}\ mod\ n^2\right)\right)^{-1}\ mod\ n$,where function $L$is defined as $L(u) = \frac{u-1}{n}$

Note that the notation $\frac{a}{b}$does not denote the modular multiplication of a times the modular multiplicative of $b$but rather the quotient of a divided by b i.e., the largest integer value $v \geq 0$ to satisfy the relation $a \geq vb$

- The public encryption key is (n, g)
- The private (decryption) key is(λ, μ)

If using p, q of equivalent length a simpler variant of the above key generation steps would be set $g = n + 1, \lambda = \varphi(n)$and $\mu = \varphi(n)^{-1} mod\ n$,where$\varphi(n) = (p-1)(q-1)$

- **Encryption**
  1. let$m$ be a message to be encrypted where $m \epsilon \mathbb{Z}_n$
  2. select random r where $r \epsilon \mathbb{Z}^*_n$
  3. Compute cipher text as: $c = g^m . r^n mod\ n^2$
- **Decryption**
  1. Let c be the cipher text to decrypt, where $c \in \mathbb{Z}^*_{n^2}$
  2. Compute the plaintext message as: $m = L\big(c^{\lambda} mod\ n^2\big).\mu\ mod\ n$

V. CONCLUSION

We have introduced the MANET network and classification of routing used in MANET. The communication in MANET has two phases i.e. route discovery and data transmission. The security requirements for both phases are different. The NCPR protocol significantly reduces the routing overhead. To provide security different cryptpographic techniques can be used. Some systems that exist to satisfy seurity requirements are discussed in review. The Paillier cryptography is public key cryptosystem that provide the security to data transmission phase.

REFERENCES

[1] XinMingZhang, En Bo Wang, Jing Jing Xia, Dan Keun Sung (2013) "A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad Hoc Networks" IEEE transactions on Mobile Computing, Vol. 12,.

[2] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing", IETF RFC 3561, 2003.

[3] PanagiotisPapadimitratos and Zygmunt J. Haas," Secure Data Transmission in Mobile Ad Hoc Networks" ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003

[4] Wenjia Li and Anupam Joshi," Security Issues in Mobile Ad Hoc Networks" Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County.

[5] Seung Yi, Prasad Naldurg, Robin Kravets," SecurityAware Ad hoc Routing for Wireless Networks"

[6] M. G. Zapata and N. Asokan, "Securing Ad hoc routing protocols" In wise'02 proceedings of ACM workshop on wireless security ACM press 2002.

[7] Lidong Zhou and Zygmunt J. Haas," Securing Ad Hoc Networks" Cornell University IEEE Network –November/ December 1999 .

[8] Michael O'Keeffe," The Paillier Cryptosystem" Mathematics Department April 18, 2008

[9] Hongmei Deng, Wei Li, and Dharma P. Agrawal," Routing Security in Wireless Ad Hoc Networks" IEEE Communications Magazine • October 2002

[10] Jianmin Chen and Jie Wu," A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks"

[11] S. Kent and R. Atkinson., "Security Architecture for the Internet Protocol," IETF RFC 2401, Nov. 1998.

[12] D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet Security Association and Key Management Protocol," IETF RFC 2408, Nov. 1998.

[13] J. Lundberg, "Routing security in ad hoc network",2000.

[14] H. Deng "Routing security in wireless ad hoc networks",2002.

[15] M.Jakobsson,S.Wetzel and B.Yener, "Stealth attacks on ad hoc wireless networks in proceedings of VTC,2003.