International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

An Efficient Secure Ad Hoc Routing Protocol for Optimize the Performance of Mobile Ad Hoc Network (MANET)

Md. Torikur Rahman

Lecturer, Department of Computer Science & Engineering, Uttara University, Dhaka, Bangladesh

How to cite this paper: Md. Torikur Rahman "An Efficient Secure Ad Hoc Routing Protocol for Optimize the Performance of Mobile Ad Hoc Network (MANET)" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.409-416, URL: https://www.ijtsrd.com/papers/ijtsrd23727.pdf

IJTSRD23727

ABSTRACT

Nowadays Mobile Ad Hoc Network (MANET) is an emerging area of research to provide various communication services to the end users. Recently the fields of MANET have yielded more and more popularity and thus MANET have become a subject of great interest for the researchers to enforce research activities. One of the main challenges in Mobile ad hoc network is of searching and maintaining an effective route for transporting data information securely. Security and privacy are indispensable in various communications for successful acceptance and deployment of such a technology. Mobile Ad Hoc Network (MANET) is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. There is an increasing trend to adopt mobile ad hoc networking for commercial uses; however, their main applications lie in military, tactical and other security-sensitive operations. In these and other applications of mobile ad hoc networking, secure routing is an important issue. Thinking of this, I proposed an efficient secure ad hoc routing protocol for optimize the performance of MANET which will more efficient in terms of time delay, packet drop and packet delivery fraction in mobile ad hoc network. The proposed protocol can employ an integrated approach of digital signature and encryption techniques to achieve the security goals like message integrity, data confidentiality and end to end authentication at IP layer. Together with existing approaches for securing the physical and MAC layer within the network protocol stack, the proposed secure routing protocol can provide a foundation for the secure operation of an ad hoc network.

Keywords: *MANETs; ZRP; DoS; Encryption; Hashing*

INTRODUCTION

A mobile ad hoc network (MANET) sometimes called a wireless ad hoc network or a mobile mesh network is a wireless network, comprised of mobile computing devices (nodes) that use wireless transmission for communication, without the aid of any established infrastructure or centralized administration such as a base station or an access point [1, 2, 3, 4]. Unlike traditional mobile wireless networks, mobile ad hoc networks do not rely on any central coordinator but communicate in a self-organized way. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those far apart rely on other nodes to relay messages as routers. In ad hoc network each node acts both as a host (which is capable of sending and receiving) and a router which forwards the data intended for some other node. Ad hoc wireless networks can be deployed quickly anywhere and anytime as they eliminate the complexity of infrastructure setup.

Applications of ad hoc network range from military operations and emergency disaster relief, to commercial uses such as community networking and interaction between attendees at a meeting or students during a lecture. Most of these applications demand a secure and reliable communication.

Mobile wireless networks are generally more vulnerable to information and physical security threats than fixed wired networks. Vulnerability of channels and nodes, absence of infrastructure and dynamically changing topology, make ad hoc networks security a difficult task [4]. Broadcast wireless channels allow message eavesdropping and injection (vulnerability of channels). Nodes do not reside in physically protected places, and hence can easily fall under the attackers' control (node vulnerability). The absence of infrastructure makes the classical security solutions based on certification authorities and on-line servers inapplicable. In addition to this, the security of routing protocols in the MANET dynamic environment is an additional challenge.

Most of the previous research on ad hoc networking has been done focusing only upon the efficiency of the network. There are quite a number of routing protocols proposed [5, 6, 7] that are excellent in terms of efficiency. However, they were generally designed for a non-adversarial network setting, assuming a trusted environment; hence no security mechanism has been considered. But in a more realistic setting such as a battle field or a police rescue operation, in which, an adversary may attempt to disrupt the communication; a secure ad hoc routing protocol is highly desirable.

The unique characteristics of ad hoc networks present a host of research areas related to security, such as, key management models, secure routing protocols, instruction detection systems and trust based models. This research work is based on the research done in the area of secure routing.

AD HOC NETWORKING

Mobility is becoming increasingly important for users of computing systems. Technology has made possible smaller, less expensive and more powerful wireless communicating devices and computers. The necessary mobile computing support is being provided in some areas by installing base stations and access points. Mobile users can maintain their connectivity by accessing this infrastructure from home, from the office, or while on the road.

Such mobility support is not available in all locations where mobile communication is desired. If mobile users want to communicate in the absence of a support structure, they must form an ad hoc network.

A. Mobile Ad Hoc Networks

A mobile ad hoc network (MANET), sometimes called a wireless ad hoc network or a mobile mesh network is a wireless network, comprised of mobile computing devices (nodes) that use wireless transmission for communication, without the aid of any established infrastructure or centralized administration such as a base station in cellular network or an access point in wireless local area network [1, 2, 3, 4]. The nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Unlike traditional mobile wireless networks, mobile ad hoc networks do not rely on any central coordinator but communicate in a self-organized way. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those far apart rely on other nodes to relay messages as routers. In ad hoc network each node acts both as a host (which is capable of sending and receiving) and a router which forwards the data intended for some other node. Hence it is appropriate to call such networks as "multi-hop wireless ad hoc networks". Figure 1 shows an example of mobile ad hoc network and its communication technology.

As shown in Figure 1, an ad hoc network might consist of several home-computing devices, including laptops, cellular phones, and so on. Each node will be able to communicate directly with any other node that resides within its transmission range. For communicating with nodes that reside beyond this range, the node needs to use intermediate nodes to relay the messages hop by hop.

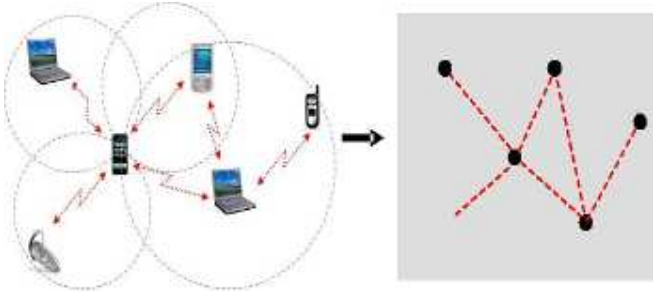

Figure 1: A Typical Mobile Ad Hoc Network

B. Manet Applications

Ad hoc wireless networks, due to their quick and economically less demanding deployment, find applications in several areas [1]. Some of these include:

- Military applications, such as establishing communication among a group of soldiers for tactical operations when setting up a fixed wireless communication infrastructure in enemy territories.
- Emergency systems, for example, establishing communication among rescue personnel in disaster-affected area that need quick deployment of a network.
- Commercial uses such as community networking and interaction between attendees at a meeting or students during a lecture.
- Collaborative and distributed computing.
- Wireless mesh networks and wireless sensor networks

EXISTING ROUTING APPROACHES IN MANET

There are generally categorized as table-driven or proactive, on-demand or reactive and hybrid routing protocols.

- Table-driven or Proactive Protocols: Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals [9]. Representative proactive protocols include:

I. Destination-Sequenced Distance-Vector (DSDV) routing
II. Clustered Gateway Switch Routing (CGSR)
III. Wireless Routing Protocol (WRP)
IV. Optimized Link State Routing (OLSR) [10]

- On-demand or Reactive Protocols: Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Once a route has been established, it is maintained by the node until either the destination becomes inaccessible or until the route is no longer used or has expired [8]. Representative reactive routing protocols include:

1. Dynamic Source Routing (DSR)
2. Ad hoc On Demand Distance Vector (AODV) routing
3. Temporally Ordered Routing Algorithm (TORA)
4. Associativity Based Routing (ABR)

- Hybrid Routing Protocols: Purely proactive or purely reactive protocols perform well in a limited region of network setting. However, the diverse applications of ad hoc networks across a wide range of operational conditions and network configuration pose a challenge for a single protocol to operate efficiently. For example, reactive routing protocols are well suited for networks where the call-to-mobility ratio is relatively low. Proactive routing protocols, on the other hand, are well suited for networks where this ratio is relatively high. The performance of either class of protocols degrades when the protocols are applied to regions of ad hoc networks space between the two extremes [6]. Researchers advocate that the issue of efficient operation over a wide range of conditions can be addressed by a hybrid routing approach, where the proactive and the reactive behavior is mixed in the amounts that best match these operational conditions. Representative hybrid routing protocols include:

a. Zone Routing Protocol (ZRP)
b. Zone-based Hierarchal Link state routing protocol (ZHLS)

SECURITY IN MOBILE AD HOC NETWORKS

Security Goals: To secure a Mobile Ad Hoc Network, a security protocol must satisfy the following attributes: confidentiality, integrity, availability, authenticity [11].

- Confidentiality ensures that classified information in the network is never disclosed to unauthorized entities. Sensitive information, such as strategic military decisions or location information requires confidentiality.
- Integrity guarantees that a message being transferred between nodes is never altered or corrupted. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network [12].
- Availability implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system. Availability of a network can be tempered for example by dropping off packets and by resource depletion attacks.
- Authenticity is a network service to determine a user's identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network [13].
- Finally, non-repudiation ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

Security Attacks

- Passive attacks: A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it [15]. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected.
- Active attacks: An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external.
- Man-in-the-Middle Attack: In this attack, a malicious node impersonates the receiver with respect to the sender, and the sender with respect to the receiver, without having either of them realize that they have been attacked with an intension to read or modify the messages between two parties.
- Information disclosure Attack: In this, a compromised node may leak confidential information to unauthorized nodes in the network. Such information may include information regarding the network topology, geographic location of nodes or, optimal routes to unauthorized nodes in the network.
- Attacks using Modification: This attack disrupts the routing function by having the attacker illegally modifying the content of the messages. Some of the attacks involving packet modification are given below:

Misrouting Attack: In the misrouting attack, a non-legitimate node redirects the routing message and sends data packet to the wrong destination.

Denial of service (DoS) attack: In this type of attack, an attacker attempts to prevent legitimate and authorized users of services offered by the network from accessing those services. A DoS attack can be carried out in many ways and against any layer in the network protocol stack.

A. Security Mechanisms and Solutions

Having seen the various kinds of attacks possible on ad hoc routing, I look at various techniques employed to overcome these attacks. There can be two types of security mechanisms: preventive and detective. Preventive mechanisms are typically based on message encryption techniques, while detective mechanisms include the application of digital signature and cryptographic hash functions.

Message Encryption: Message encryption is the technique of transforming a message into a disguised message which no unauthenticated individual can read, but which can be restored in its genuine form by an intended receiver [14]. The plaintext is converted into cipher text by the process of encryption, which can be done by the use of certain algorithms or functions. The reverse process is termed as decryption [16]. The process of encryption and decryption are governed by keys, which are small amount of information used by the cryptographic algorithms. There are two types of encryption techniques: symmetric key and asymmetric key (or public key). Symmetric key cryptosystem uses the same key (the secret key) for encryption and decryption of a message, whereas asymmetric key cryptosystems use one key (the public key) to encrypt a message and another key (the private key) to decrypt it. Public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used for decryption purpose [17]. Even if attacker comprises a public key, it is virtually impossible to deduce the private key. Symmetric key algorithms are usually faster to execute electronically than the asymmetric key algorithms. Asymmetric key algorithm is comparatively slower process than symmetric but could be a great use in the establishment of a secure network system. Here I use the asymmetric-key cryptography for my proposed network.

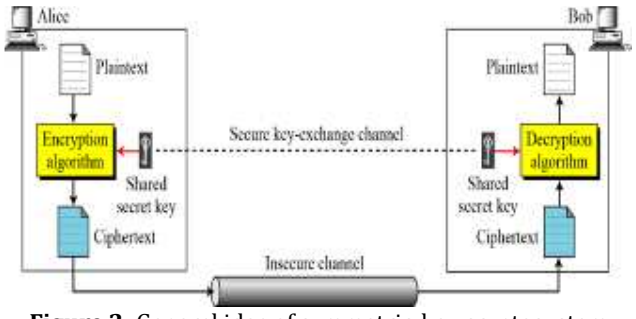

Figure 2: General idea of symmetric-key cryptosystem

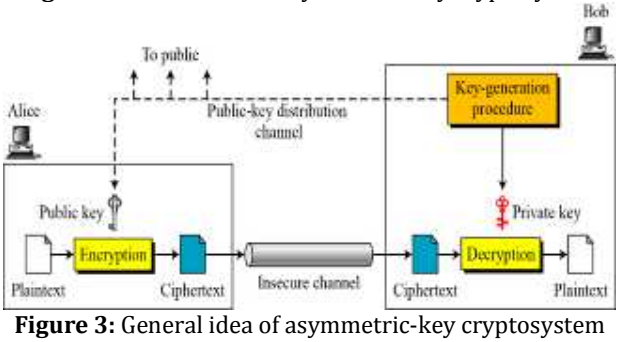

Figure 3: General idea of asymmetric-key cryptosystem

Digital signature and Hashing: The process of encryption only ensures the confidentiality of the message being sent. Digital signature is a technique by which one can achieve the other security goals like message integrity, authentication and non-repudiation. In digital signature, a block of data or a sample of the message (called a message digest) represents a private key. When this message digest is encrypted with the owner's private key, then a digital signature is created. This digital signature is then added at the end of each message that is to be sent to the recipient [18]. The recipient decrypts the message using the owner's public key and thus verifies that the message digest is correct and the message has come from the genuine sender. The process of digital signature is outlined below:

- Sender generates a message.
- Sender creates a "digest" of the message.
- Sender encrypts the message digest with his/her private key for authentication. This encrypted message digest is called digital signature.
- Sender attaches the digital signature to the end of the message that is to be sent.
- Sender encrypts both the message and signature with the recipient's public key.
- The recipient decrypts the entire message with his/her private key.

Thus, the recipient verifies the digest for accuracy.

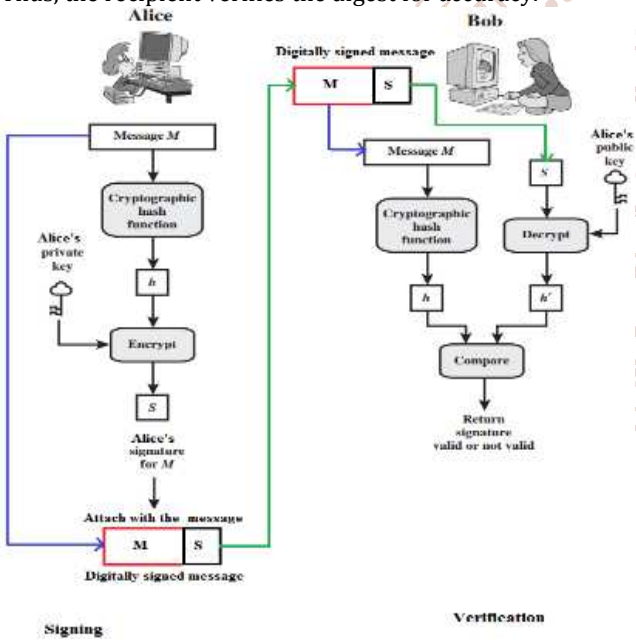

Figure 4: Illustration of digital signature process

Hashing can be used for the digital signature process especially when the message is long. In this the message is passed through an algorithm called cryptographic hash function or one-way hash function before signing. Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. A hash value (or simply hash), also called a message digest, is a number generated from a string of text. The hash is substantially smaller than the text itself. In hashing, a fixed-length message digest is created out of a variable-length message. The digest is normally much smaller than the message. It plays a vital role in security system that creates a unique, fixed-length signature for a message or data set. People commonly use them to compare sets of data. Since a hash is unique to a specific message, even minor changes to that message result in a dramatically different hash. Therefore, it is very resistant to tampering.

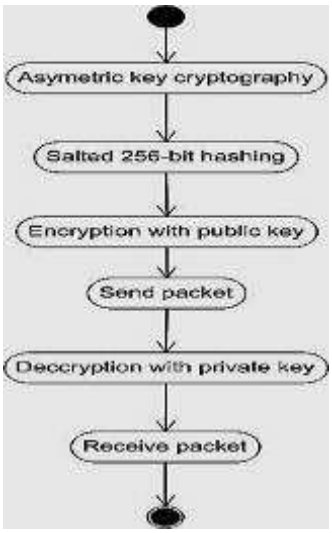

Figure 5: Flowchart of overall Security Mechanisms

B. Requirements for a Secure Routing Protocol

Considering the attacks, I list here the fundamental requisites of a secure routing protocol for Mobile ad hoc networks. They are- Routing messages cannot be altered in transit, except according to the normal functionality. Route signaling cannot be spoofed. Fabricated routing messages cannot be injected into the network. Routing loops cannot be formed through malicious action. Routes cannot be redirected from the shortest path by malicious action. Unauthorized nodes should be excluded from route computation and discovery. The network topology must not be exposed by the routing messages either to adversaries or to authorized nodes.

PROPOSED PROTOCOL OVERVIEW

Neither a pure proactive nor a pure reactive approach provides a full solution for secure ad hoc routing that performs efficiency across a wide range of operational requisites and network configuration. For a complete, efficient and implementable solution for secure routing is highly desirable that can operate well on diverse applications of ad hoc networks. I use hash function in MANET.

The proposed protocol is developed on the concept of Zone Routing Protocol (ZRP). It is a hybrid routing protocol that is comprised of the best features of both proactive and reactive approaches and adds its own security mechanisms to perform secure routing. The reasons for selecting ZRP as the basis of my protocol are as follows:

ZRP is based on the concept of routing zones, a restricted area, and it is more feasible to apply the security mechanisms within a restricted area than in a broader area that of the whole network [19]. Since the concept of zones separate the communicating nodes in terms of interior (nodes within the zone) and exterior (nodes outside the zone) nodes, certain information like network topology and neighborhood information etc. can be hidden to the exterior nodes, in case of a failure, it can be restricted to a zone.

Like ZRP the proposed protocol performs routing in terms of intra-zone and inter-zone routing. However, it differs from

ZRP in security aspects. In ZRP where there is no security consideration, the proposed protocol is designed to address all measure security concerns like end to end authentication, message/packet integrity and data confidentiality during both intra and inter-zone routing.

Table 1: Table of Notations

Notation	Description
SKx	Signature Key of node X
VKx	Signature verification key for node X
EKx	Encryption Key for node X
DKx	Decryption Key of node X
[d] SKx	Packet d signed with SKx, this can be only verified using VKx
[d]EKx	Message d encrypted with EKx, this can be only decrypted with DKx
[d]—b	b is appended to the packet containing d
CERTx	Public key certificate of X
IPx	IP address of X
T	Time stamp
E	Certificate expiration time
Nx	Nonce issued by node X
SKREQ	Session Key Request packet identifier
SKREP	Session Key Reply packet identifier
SRD	Secure Route Discovery packet identifier
SRR	Secure Route Reply packet identifier
ERR	Error packet identifier

Certification Process: The proposed Protocol requires the presence of trusted certification servers called the certification authorities (CAs) in the network. The CAs are assumed to be safe, whose public keys are known to all valid CNs. Keys are generated apriori and exchanged through an existing, perhaps out of band, relationship between CA and each CN. Before entering the ad hoc network, each node requests a certificate from its nearest CA. Each node receives exactly one certificate after securely authenticating their identity to the CA. The idea is depicted in Figure 6. The methods for secure authentication to the certificate server are numerous and hence it is left to the developers; a significant list is provided by [14].

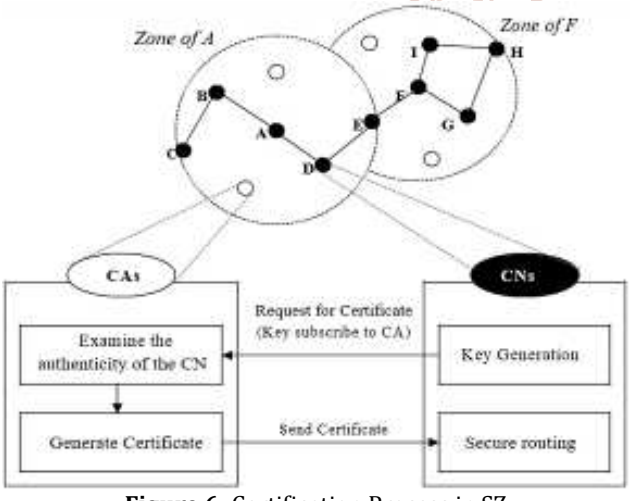

Figure 6: Certification Process in SZ

The Secure Routing Algorithm: This section describes the secure intra-zone and inter-zone routing in details. I consider the network in Figure 7 for the illustration.

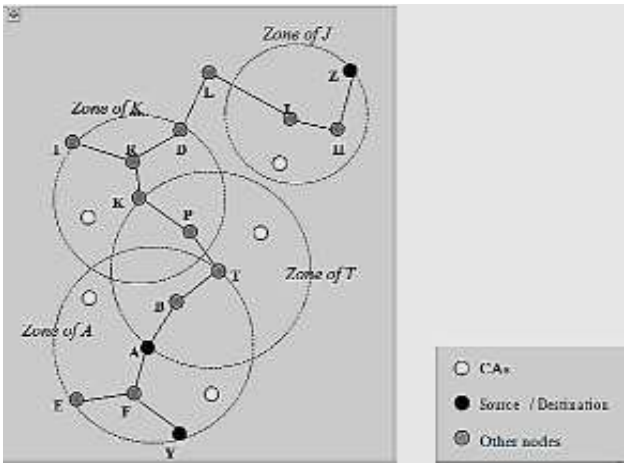

Figure 7: Intra-zone and Inter-zone destinations of node A (zone radius = 2)

Secure Intra-Zone Routing (IARP): The Intra zone Routing Protocol (IARP) is a limited scope proactive routing protocol, which is used to support a primary global routing protocol. The routing zone radius shows the scope of the proactive part, the distance in hops that IARP route updates relayed. IARP's proactive tracking of local network connectivity provides support for route acquiring and route maintenance. First routes to local nodes are immediately available, avoiding the traffic overhead and latency of a route discovery. Here is the intra-zone routing activity overview of the network.

Figure 8: Basic activity diagram of Secure Intra-zone routing

Secure Inter-Zone Routing (IERP): The Inter-Zone Routing Protocol (IERP) is the global re-active routing component of the Zone Routing Protocol (ZRP). IERP adapts existing reactive routing protocol implementations to take advantage of the known topology of each node surrounding R-hop neighborhood (routing zone), provided by the Inter-zone outing Protocol (IARP). The availability of routing zone routes allows IERP to suppress route queries for local destinations. Here is the inter-zone routing activity overview of the network

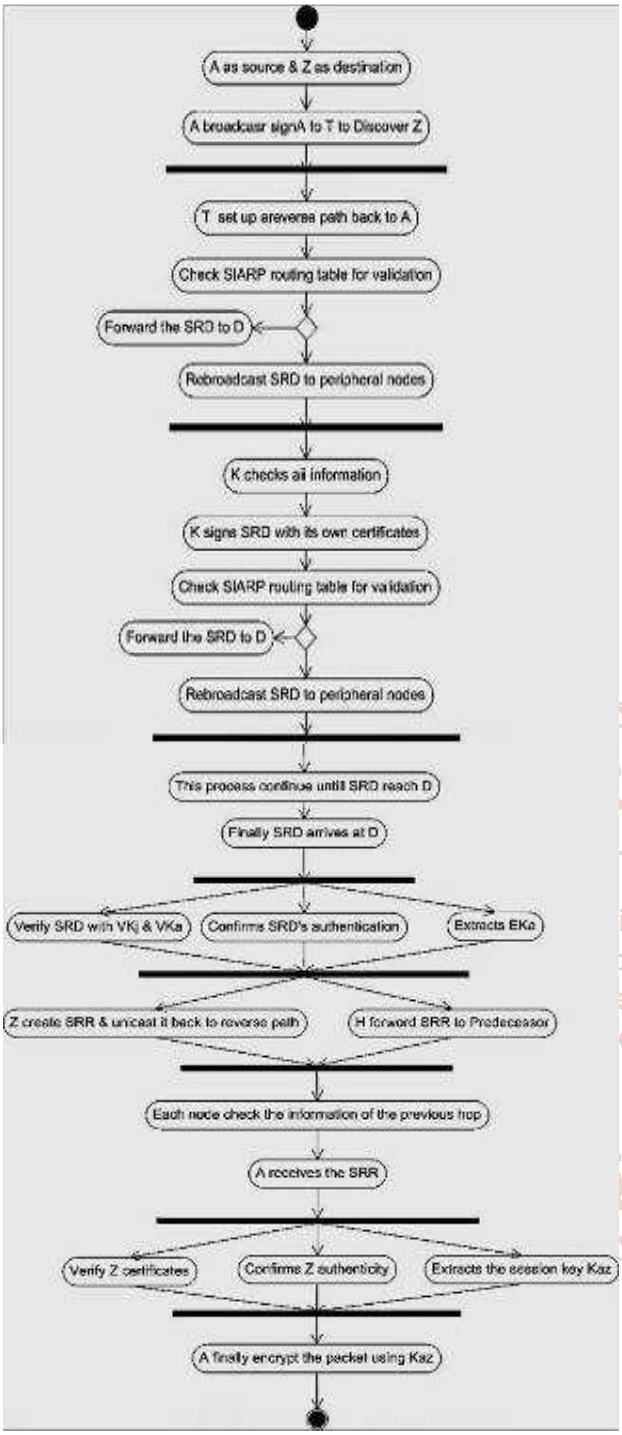

Figure 9: Basic activity diagram of Secure Inter-zone routing

A. Analysis of Proposed Secure Routing Protocol

In this section, I analyze the security aspects of proposed Routing Protocol by evaluating its robustness in the presence of attacks mentioned in Section 3.3. Proposed Protocol can prevent against all types of attacks that include information disclosure, impersonation, modification, fabrication and replay of packets caused by both an external advisory and an internal compromised node.

Prevention from Information Disclosure: No hop count information is present in the SRD or SRR packets. This prevents an external advisory or an internal compromised node from getting any kind of information about the network topology. Topology information is restricted to nodes within a zone. This is harmless as nodes accept packets only after verifying the sender's signature. Further all the data packets and the control packets that contain the session key are encrypted which ensures the confidentiality.

Attacks involving impersonation: Proposed Protocol participants, accept only those packets that have been signed with a certified key issued by a CA. In intra-zone routing since the SKREQs and SKREPs can only be signed by an authenticated source with its own private signature key, nodes can't impersonate (spoof) other nodes. Inter-zone routing follows hop-by-hop authentication during route discovery and end-to-end authentication during the route reply phase. So it is impossible for an external node or an internal compromised node to impersonate an intermediate node during inter-zone routing. Further since the SRD packet is signed by the source node using its private key, it guarantees that only the source can initiate a route discovery process. Similarly, the SRR packets include the destination's certificate and signature, ensuring that only the destination can respond to the route discovery. This prevents attacks where the source, the destination or any intermediate nodes are spoofed e.g. man-in-the-middle attack and sybil attack [15].

Routing message Modification: Proposed Protocol specifies that all fields of LSPs, SRD and SRR packets remain unchanged between the source and the destination. Since all packets are signed by the initiating node, any alterations in transit would be immediately detected by intermediate nodes along the path, and the altered packets would be subsequently discarded. Repeated instances of altering packets could cause other nodes to exclude the errant node from routing. Thus, modification attacks like redirection of routing messages and DoS attacks are prevented.

Fabrication of messages: Messages can be fabricated only by the internal compromised nodes with certificates. In that case, Proposed Protocol does not prevent fabrication of routing messages, but it does offer a deterrent by ensuring non-repudiation. A node that continues to inject false messages into the network may be excluded from future route computation.

Replay Attacks: Replay attacks like tunneling and wormhole attacks are prevented by including a nonce and a timestamp with routing messages.

SIMULATION FOR SECURE ROUTING PROTOCOL

A. Simulation Issues

- Average packet delivery fraction: This is the fraction of the data packets generated by the sources that are delivered to the destination.
- Average route acquisition latency: This is the average delay between the sending of a secure route discovery packet by a source for discovering a route to a destination and the receipt of the first corresponding route reply.
- Percentage of Packets Dropped that passed through Malicious Nodes: This metric indicates the percentage of total packets dropped that traverse malicious nodes when using each routing protocol. Assuming that all the packets that pass through a malicious or compromised node were altered, this metric can be calculated as follows:

$$\%\ of\ Packets\ Dropped\ that\ passed\ through\ Malicious\ Nodes = \left(\frac{No.\ of\ packets\ dropped\ by\ the\ benign\ nodes\ that\ are\ previously\ generated\ by\ or\ passed\ through\ any\ malicious\ node\ in\ the\ network}{Total\ number\ of\ packets\ communicated} \right) X\ 100$$

B. Simulation Result

Average Packet Delivery Fraction: Figure 10 shows the observed results for average packet delivery fraction for both the 10 and 20 node networks. As shown in the figure 10, the packet delivery fraction obtained using proposed algorithm is above 96% in all scenarios and almost identical to that obtained using ZRP. This suggests that proposed algorithm is highly effective in discovering and maintaining routes for delivery of data packets, even with relatively high node mobility.

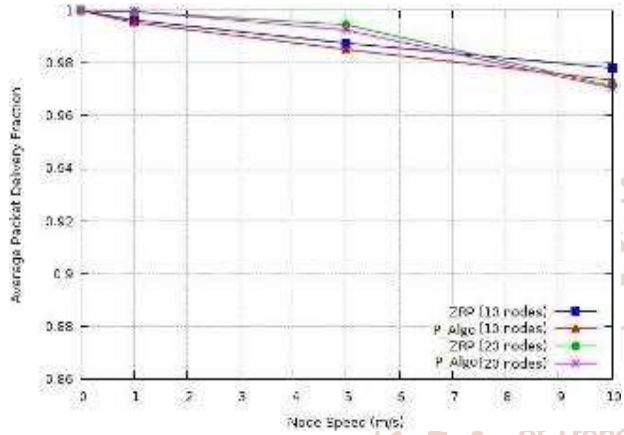

Figure 10: Simulation Results – Average Packet Delivery Fraction

Average Route Acquisition Latency: Figure 11 shows that the average route acquisition latency for Proposed Protocol is approximately 2 times as that of ZRP. For example, for 10 nodes moving at 5 m/s, it is 60ms as compared to 100ms for ZRP, while for 20 nodes moving at 10 m/s, it is nearly 135ms as compared to 75ms as in the case of ZRP. While processing proposed algorithm control packets, each node has to verify the digital signature of the previous node, and then replace this with its own digital signature, in addition to the normal processing of the packet as done by ZRP. This signature generation and verification causes additional delays at each hop, and so the route acquisition latency increases.

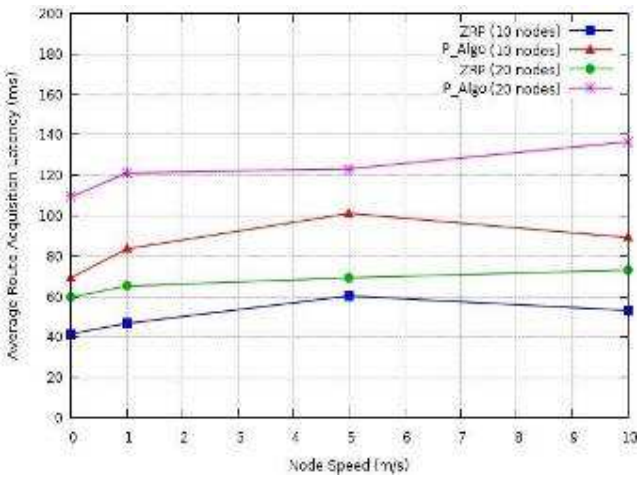

Figure 11: Simulation Results – Average Route Acquisition Latency

Percentage of Packets Dropped: As shown in the Figure 12, when using Proposed algorithm, a much larger fraction of packets that passed through malicious nodes were dropped, as compared to that of ZRP. These results show that about 50% of packets that were possibly altered by malicious nodes in the network remained undetected and could potentially make their way through authentic nodes when using ZRP, as compared to the proposed protocol. This is a significant increase in the degree of security level.

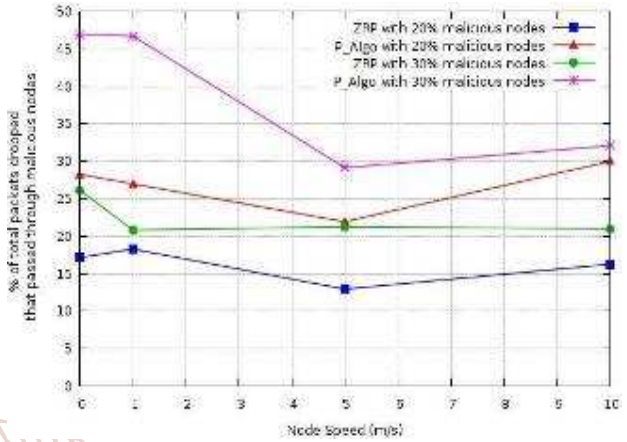

Figure 12: Simulation Results – Percentage of Packets Dropped

CONCLUSION

In this research work, I have considered the routing approaches in mobile ad hoc networks from the security viewpoint. I have analyzed the threats against ad hoc routing protocols and presented the requirements that need to be addressed for secure routing. I have presented the design and analysis of a new secure routing protocol for mobile ad hoc networks which is hybrid in nature and based on the concept of zone routing protocol (ZRP). It provides a solution for secure routing in an open and managed-open environment. In designing the proposed protocol, I carefully fit the inexpensive cryptographic primitives to each part of the protocol functionality to create an efficient protocol that is robust against multiple attacks in the network. The proposed protocol gives a better solution towards achieving the security goals like message integrity, data confidentiality and message authentication, by taking an integrated approach of digital signature and encryption techniques. The effectiveness of the proposed protocol in terms of time delay, packet drop and packet delivery fraction in mobile ad hoc networks can redirect a new way towards optimization development in network communication. Comparing others, it can be said that the working process of the proposed scheme is far better. With a view to different measurements, the proposed secure routing protocol for mobile ad hoc network will be effective for pursuing an optimized platform.

References

[1] C. Siva Ram Murthy and B. S Manoj, "Ad Hoc Wireless Networks, Architecture and Protocols", Prentice Hall PTR, 2004.

[2] Stefano Basagni, Macro Conti, Silvia Giordano and Ivan Stojmenovic, "Mobile Ad Hoc Networks" , IEEE press, A john Wily & Sons, INC. publication, 2003

[3] George Aggelou, "Mobile Ad Hoc Networks", 2nd edition, Mc GRAW Hill professional engineering, 2004

[4] Imrich Chlamtac, Marco Conti, Jenifer J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challanges", Elsevier Network Magazine, vol. 13, pages 13-64, 2003

[5] E. M. Belding-Royer and C. K. Toh, "A review of current routing protocols for ad-hoc mobile wireless networks", IEEE Personal Communications Magazine, pages 46–55, April 1999.

[6] Haas Z. J., Pearlman M. R., and Samar P., "The Zone Routing Protocol (ZRP)", IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[7] M. Joa-Ng and I. T. Lu, "A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks," IEEE journal on Selected areas in Communications, vol. 17, no. 8, pp. 1415- 1425, August 1999

[8] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing", In IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, Feb. 1999.

[9] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Comp. Commun. Rev., Oct. 1994, pp. 234–44.

[10] P. Jacquet, P. Muhlethaler, A. Qayyum, "Optimized Link State Routing Protocol", Internet Draft, draft-ietf-manetolsr- 00.txt, November 1998.

[11] D. B. Johnson, D.A. Maltz, "Dynamic source routing in adhoc wireless networks", in: T. Imielinski, H. Korth (Eds.), Mobile Computing, Kluwer Academic Publishers, Dordrecht, 1996, pp. 153–181.

[12] L. Zhou and Z. J Haas, "Securing Ad Hoc networks," IEEE Network Magazine, vol. 13, no. 6, December 1999

[13] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing Security in Ad Hoc Wireless Networks," Network Security, S. Huang, D. MacCallum, and D. -Z. Du (eds.), Springer, 2008.

[14] Behrouz A. Forouzan, "Cryptography and Network Security", Special Indian Edition, Tata McHill publication, 2007

[15] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks: Analysis & Defenses, Proc. of the 3rd Intl. Symp. on Information Processing in Sensor Networks, 2004

[16] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure routing protocol Resilient to Byzantine failures", Proceedings of ACM workshop on wireless security 2003, September 2003

[17] J. J. Tardo and K. Algappan, "SPX: Global authentication using public key certificates", In Proceedings of the 1991 IEEE Symposium on Security and Privacy, pages 232–244, Oakland, CA USA, May 1991. IEEE Computer Society Press.

[18] P. Michiardi, R. Molva, "Ad hoc networks security", in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003.

[19] Jan Schaumann, "Analysis of Zone Routing Protocol", Course CS765, Stevens Institute of Technology Hoboken, New Jersey, USA, 8th December 2002.