Proactive Bai's Secret Sharing Scheme for AOMDV Routing Protocol for Secured Communication in MANET

C. Chandrasekar[*] , Lt. Dr. S. Santhosh Baboo[α]
[*]Research Scholar , Computer Science, Manonmaniam Sundaranar University, Tirunelveli – 627 012.
[α]Reader, P.G. and Research, Dept of Computer Science, D. G. Vaishnav College, Chennai – 600 106.

Abstract--- The amount of applications in Wireless networks is developing continuously. And hence the need for security in wireless communication is also developing constantly with the development of Wireless communication particularly in MANET. Security is of a great concern in the present wireless communication. It is essential to provide security to the network from the attackers and their security attacks. With the purpose of providing a secured communication, it is crucial that routing protocol should be secured adequately against the the security attackers. In this paper, integrated Proactive Bai's Secret Sharing Scheme with Ad-hoc On-demand Multipath Distance Vector routing protocol (PSS-AOMDV) for secured communication. In order to protect a secret from being exposed by adversary attacks, shares are periodically updated in an effective way using proactive secret sharing scheme. To evaluate the performance of the proposed PSS-AOMDV, it is compared against AOMDV and SAOMDV (AOMDV with Shamir's Secret Sharing Scheme) on the basis of number of packets received and the packet delivery ratio against the introduction of malicious nodes respectively.

Keywords--- Mobile Ad-hoc Networks, Multihop Wireless Networks, Proactive Bai's Secret Sharing Scheme, Ad-hoc On-Demand Multipath Distance Vector (AOMDV),

I. INTRODUCTION

WIRELESS applications are growing rapidly in the present wireless environment. Due to the over growth of the wireless applications, security is also becoming more important especially in Mobile Ad-hoc NETwork (MANET). MANET is a mobile, multihop wireless network that does not depend on any predefined infrastructure. MANETs are featured by active topologies because of their uncontrolled node mobility, inadequate and uneven shared wireless channel bandwidth and wireless devices constrained by battery power. The major challenge in MANETs is to intend dynamic routing protocols that are proficient with very less overhead.

Security in MANETs is of a major concern and it has become an active area of research. To prevent a variety of attacks in MANETs has been a challenging issue for researchers as MANETs has been widely used in military applications, emergency rescue operations, in confidential video conferencing, etc. A MANET is an automatic network which is fully active and spread in nature. The operations of every node are similar but the recognition of an attacker or malevolent (malicious) nodes amongst the network is a difficult task. Recently, the security for multicast routing in MANETs has also become very vital. Several security protocols have been developed under the operations of multicast [1]. However, these protocols are susceptible to several types of attacks on MANETs [2] like flooding, blackhole, wormhole, etc. Various researches are being done for handling the attacks in MANETs.

The major purpose of using routing protocols in an ad-hoc network is to facilitate the source to identify routes to destination with the cooperation of other nodes. Because of the random movement of the nodes, the network topology alters quickly and arbitrarily. Thus, the routing protocol must be capable of handling these alterations and must facilitate the nodes to find new routes to sustain connectivity. The security in MANETs [3][4] has become a serious issue mainly because of the active characteristic of the ad hoc network and because of the necessity to function efficiently with inadequate resources, including network bandwidth and the CPU processing capacity, memory and battery power (energy) of each individual node in the network. Quick and frequent routing protocol communication between nodes is very much needed [13].

Integrating secret sharing scheme with a routing protocol is new concept. Moreover, a secret sharing scheme is rather susceptible [16] when a dynamic adversary determines to break into the system before the lifetime of the secret terminates. Along with several different categories of adversary attacks, one of the most prominent ways is to categorize these attacks as:

- Passive adversary attacks
- Active adversary attacks.

Passive adversary attacks are largely resulting in spoofing data without any change or corruption to the data. On the contrary to the passive adversary attacks, the active adversary attacks are much more vulnerable in which the adversaries can steadily attempt to penetrate into a system, or it will attempt to destroy data already accumulated in the system.

In this paper, Proactive Bai's secret sharing scheme is used for the purpose of providing secured communication in MANET. The secret key sharing scheme is used in this approach as it provides assurance to the source node or the owner regarding the genuinely participating nodes in the network.

Ad-hoc On-Demand Multipath Distance Vector (AOMDV) is one of the potential routing protocols for maintaining security. Several intruders are very much interested in attacking the nodes or route to steal the data packets [15]. In order to provide more security, Proactive Bai's secret sharing scheme is integrated with AOMDV for secured communication (PSS-AOMDV). In PSS-AOMDV, only the authorized users are allowed to take part in the communication and thereby the intruders are not allowed to attack the system.

II. Literature Survey

MANETs has several kinds of security issues, caused by their nature of collaborative and open systems and by limited availability of resources. In this paper, Cerri et al., [5] consider a Wi-Fi connectivity data link layer as a fundamental technique and concentrates on routing security. The author discusses the implementation of the secure AODV protocol extension, which comprises of alteration policies aimed at enhancing its performance [14]. The author proposed an adaptive technique that adjusts SAODV behavior. Furthermore, the author examined the adaptive technique and another approach that delays the verification of digital signatures. This paper sums up the experimental results collected in the prototype design, implementation, and tuning.

Li Bai et al., [6] proposed a strong (k, n) threshold-based ramp secret sharing scheme with k access levels. The secrets are the elements represented in a square matrix. The secret matrix S can be shared with n different users by means of a matrix projection technique in which: (a) any subset of k users can work together to reconstruct the secret and (b) any subset of $(k-1)$ or fewer users cannot partly identify the secret matrix. The essential benefits are its large compression rate on the size of the shares and its strong protection of the secrets.

Perlman proposed a link state routing protocol [7] that attains Byzantine strength. Though, the protocol is extremely forceful, it needs a very high operating cost associated with public key encryption. Zhou and Haas [8] chiefly describe key management in their paper to provide security to ad hoc networks. The author devotes a part to secure routing, but in essence concludes that “nodes can defend routing data in the similar way they protect data traffic”. They also examine that denial-of-service attacks against routing will be considered as damage and it is routed around. Certain research has been done to secure ad hoc networks by means of misbehavior detection approaches. This technique has two major problems: Initially, it is fairly likely that it will be not possible to discover various kinds of misbehaving; and secondly, it has no real means to assure the integrity and authentication of the routing messages.

Multipath routing diminishes the penalty of security attacks obtaining from collaborating malevolent nodes in MANET, by increasing the number of nodes that an opponent must negotiate in order to take control of the communication. In this paper, various attacks that cause multipath routing protocols more susceptible to attacks than it is expected, to collaborating malevolent nodes are recognized. Kotzanikolaou et al., [9] proposed a novel On-demand Multipath routing protocol called the Secure Multipath Routing protocol (SecMR) and the author examine its security properties. The SecMR protocol can be easily combined in an extensive variety of on-demand routing protocols, such as DSR and AODV.

Herzberg et al., [16] proposed the Proactive secret sharing scheme depending on the Shamir secret sharing scheme. This scheme periodically renews the shares (without reconstructing the secret) so that it avoids an adversary attackers from obtaining the knowledge of the secret before it terminates. In order to provide security against active adversary attacks, this approach integrated the concepts in the Verifiable Secret Sharing technique.

III. Methodology

3.1. Ad hoc On-Demand Multipath Distance Vector Routing

The significant purpose of this paper is to provide a highly secured AOMDV routing protocol by incorporating Proactive Bai’s secret sharing scheme. In this section the goal is to enhance the AOMDV protocol to work out multiple disjoint loop-free paths in a route discovery. AOMDV can be implemented even in the existence of unidirectional links with other techniques to assist in discovering bidirectional paths in such circumstances [10].

AOMDV has numerous features which are similar with AODV. It is dependent on the distance vector theory and utilizes hop-by-hop routing technique. Furthermore, AOMDV also discovers routes on demand using a route discovery method. The most important variation is the amount of routes found in each route discovery. In AOMDV, RREQ transmission from the source to the target establishes multiple reverse paths both at intermediary nodes in addition to the destination. Multiple RREPs navigates this reverse route back to form multiple onward routes to the target at the source and intermediary nodes. Moreover, AOMDV also makes intermediary nodes available with alternate routes since they are established to be helpful in dropping route discovery frequency [11].

The basis of the AOMDV protocol lies in guaranteeing that multiple routes revealed are loop-free and disjoint, and in competently discovering such paths by means of a flood-based route discovery. AOMDV path revise rules, exploited locally at every node, play a major role in preserving loop-freedom and disjointness characteristics.

AOMDV depends more on the routing information previously available in the fundamental AODV protocol, thus preventing the overhead acquired in determining multiple paths. Specifically, it does not make use of any particular control packets. Additional RREPs and RERRs for multipath discovery and protection together with a small amount of extra fields in routing control packets (i.e., RREQs, RREPs, and RERRs) comprise the only extra overhead in AOMDV compared with AODV.

Disjoint Paths

In addition with continuing multiple loop-free paths, AOMDV looks for to discovering disjoint alternate routes. In order to improve the fault tolerance by means of multiple paths, disjoint paths are an essential alternative for choosing an efficient subset of alternative routes from a potentially huge set since the probability of their associated and simultaneous failure is less important when compared to overlapping alternate routes. Two categories of disjoint paths are taken into account: link disjoint and node disjoint. Link disjoint is a set of routes between a pair of nodes which does not have any mutual links, while node-disjointness in addition prevents mutual intermediary nodes.

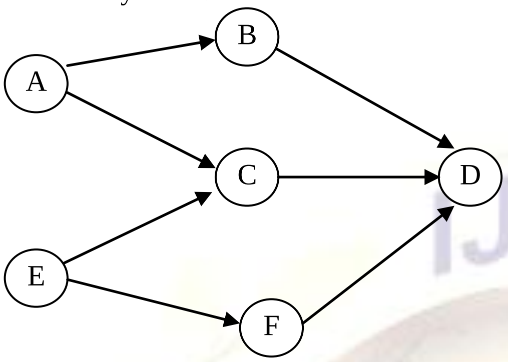

Figure 3.1: Paths maintained at different nodes to a destination possibly will not be equally disjoint.

Here D is the target. Node A has two disjoint paths to D: A – B – D and A – C – D. In the same way, node E has two disjoint paths to D: E – C – D and E – F – D. However the paths A – C – D and E – C – D are not disjoint; they share a mutual link C – D.

In this paper the AOMDV routing protocol is integrated with Proactive Bai's Secret Sharing Scheme for secured communication in MANET (PSS-AOMDV).

The following properties are satisfied in this PSS-AOMDV scheme [17],

- To renew shares without reconstructing the secret
- To disclose the secret using any k updated shares
- To avoid the secret from being revealed by using k past and present shares.

3.2. AOMDV with Proactive Bai's Secret Sharing Scheme (PSS-AOMDV)

Shamir's Secret Sharing Scheme

Shamir developed [12] the concept of a (k, n) threshold-based secret sharing technique $(k \leq n)$. The technique is to build a polynomial function of order $(k-1)$ as,

$$f(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_{k-1} x^{k-1} (mod\ p),$$

in which the value d_0 is the secret and p is a prime number. The secret shares are the pairs of values (x_i, y_i) where $y_i = f(x_i), 1 \leq i \leq n$ and $0 < x_1 < x_2 \ldots < x_n \leq p - 1$.

The polynomial function $f(x)$ is destroyed after each server P_i possesses a pair of values (x_i, y_i) in order that no single server is familiar with secret value d_0. In effect, no groups of $(k-1)$ or smaller amount of secret shares can be exploited to realize the secret d_0. Alternatively, when k or more secret shares are obtainable, at any rate k equations $y_i = f(x_i)$ with k indefinite parameters d_i's can be fixed. The distinctive solution d_0 can be solved. In addition, a Lagrange interpolation formula is normally utilized to solve the secret value d_0 as the following formula

$$d_0 = \sum_{i=0}^{k} \left(\prod_{j=1, \neq i}^{k} \frac{-x_j}{x_i - x_j} \right) y_i (mod\ p)$$

where (x_i, y_j) are any k shares for $1 \leq i \leq k$. Shamir's secret sharing scheme is considered as a perfect secret sharing scheme because knowing $(k-1)$ linear equations cannot reveal any information regarding the secret.

Proactive Secret Sharing Scheme

To periodically renew shares is an efficient method to protect a secret from being exposed by adversary attacks [16]. After the initialization of Shamir's secret sharing scheme, at the commencement of every time period, all 'honest' servers can activate an update phase in which the servers carry out a share renewal protocol. The shares calculated in period t are represented by using the superscript t, i.e., $(x_i, f^t(x_i))$, $t = 0, 1, \ldots$. Secret d_0 at time $(t-1)$ is represented as

$$d_0 = f^{(t-1)}(0).$$

The approach is to build a new $(k-1)$ random polynomial function at each updating phase as,

$$\delta(x) = a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} (mod\ p).$$

where $\delta(0) = 0$ so that $f^t(0) = f^{(t-1)}(0) + \delta(0) = d_0 + 0 = d_0$.

The share renew protocol for each server $P_i, i \in A$, during the initialization of the time period t is as follows:

P_i selects $k-1$ random numbers $\{a_{im}\}$ from Z_p for $m = 1, 2, \ldots, (k-1)$.The numbers characterize a polynomial function $\delta_i(x) = a_{i1} x + a_{i2} x^2 + \cdots + a_{i(k-1)} x^{k-1} (mod\ p)$ in Z_p.

For all additional servers P_j, P_i secretly transmits $u_{ij} = \delta_i(x_j)$ to P_j.

After decrypting u_{ji}, $\forall j \in \{1,2, \ldots, n\} P_i$ generates its new share as

$$f^t(x_i) = \left(f^{(t-1)}(x_i) + u_{1i} + u_{2i} + \cdots + u_{ni} \right) (mod\ p),$$

P_i removes all the variables it exploited except of its present secret share $y_i^t = f^t(x_i)$.

As the $\delta(x)$ function does not include any constant term, and hence any group of k or more servers can still calculate d_0 by contributing their new shares. On the other hand, a grouping of k shares using past and present shares cannot be exploited to rebuild the secret. Accordingly, the secret is protected from being exposed by the passive adversaries.

Proactive Bai's Secret Sharing Scheme

On the contrary, the matrix projection technique cannot be easily updated by exploiting the Herzberg's PSS technique [16]. For n secret shares v_i, it is necessary to establish a different technique to renew these vectors in order that the secret can be secured. In this technique, Pythagorean triples are used. The Pythagorean triples are the three integer values (Z_1, Z_2, Z_3) that satisfy the following equation [17]:

$$Z_1^2 + Z_2^2 = Z_3^2$$

For any $m \times m$ orthonormal matrix T, if $v_i^t = T v_i$ where v_i^t and v_i are the past and present shares correspondingly for $i = 1,2, \ldots, n$. Consider the matrix S^t is the projection matrix of any k renewed secret shares $\{v_i^t\}$, and the matrix S is the projection matrix of any k past secret shares $\{v_i\}$, the renewed projection matrix can be represented as,

$$S^t = TST'$$

Consider any k present shares and past shares and assume that they are v_i^t and v_i respectively, and

$$v_i^t = T \times v_i,$$

where $i = 1,2,\dots,k$.

The renewed k shares v_i^t can be used to build a matrix B^t as,

$$\begin{aligned} B^t &= [v_1^t\ v_2^t \dots v_k^t] \\ &= [Tv_1\ Tv_2 \dots Tv_k] \\ &= T[v_1\ v_2 \dots v_k] \\ &= TV \end{aligned}$$

The matrix S is the projection matrix of V, and hence,

$$S = V(V'V)^{-1}V'$$

In order to determine the renewed projection matrix S^t,

$$\begin{aligned} S^t &= B^t((B^t)'B^t)^{-1}(B^t)' \\ &= TV(V'T'TV)^{-1}V'T' \\ &= TST' \end{aligned}$$

It seems that, a renewed projection matrix S^t is correlated with the projection matrix S. While partitioning both the matrices, it is obtained that,

$$S = \begin{bmatrix} S_{11} & \vdots & S_{12} \\ \cdots & \vdots & \cdots \\ S_{21} & \vdots & S_{22} \end{bmatrix}$$

and

$$S^t = \begin{bmatrix} S_{11}^t & \vdots & S_{12}^t \\ \cdots & \vdots & \cdots \\ S_{21}^t & \vdots & S_{22}^t \end{bmatrix}$$

where matrices S_{11} and S_{11}^t represents $(m-k)\times(m-k)$ matrices, S_{12} and S_{12}^t denotes $(m-k)\times k$ matrices, S_{21} and S_{21}^t are $k\times(m-k)$ matrices, and S_{22} and S_{22}^t are $k\times k$ matrices.

In order to share the projection matrix proactively, it is to be noted that the whole projection matrix cannot be shared. Instead only the partitioned $(m-k)\times(m-k)$ matrix S_{11} can be shared. Accordingly, the original matrix S cannot be shared, but its partitioned matrix S_{11} can be shared.

IV. Experimental Results

A simulation testbed for MANET is built up to evaluate the performance of the proposed HSAOMDV against AOMDV and SAOMDV routing protocol. All these protocols were experimented over this testbed and its performance was evaluated based on different scenarios.

The values of some constraints considered during the evaluation are noted below.

Area	1500*300 meter^2
One time quantum	50 msec
Speed of the nodes	20 meters/second
Run time for the simulation	200 second
Direct Transmission Range of the nodes	250 meter
Channel capacity	1.6 Mbps

4.1. No. of Data Packets Vs No. of Malicious Nodes

In order to find the effect of malicious nodes in all these routing protocols, initially 7000 data packets are sent. From the figure 4.1, it is revealed that with the increase in the quantity of malicious nodes, the number of data packets received by AOMDV and SAOMDV decreases considerably, but the number of data packets received by PSS-AOMDV remains almost steady. It indicates that malicious nodes have only lesser consequence on the amount of data packets transmitted by PSS-AOMDV. Simultaneously, the data packets received in AOMDV and SAOMDV falls considerably with the increase in the number of malicious nodes.

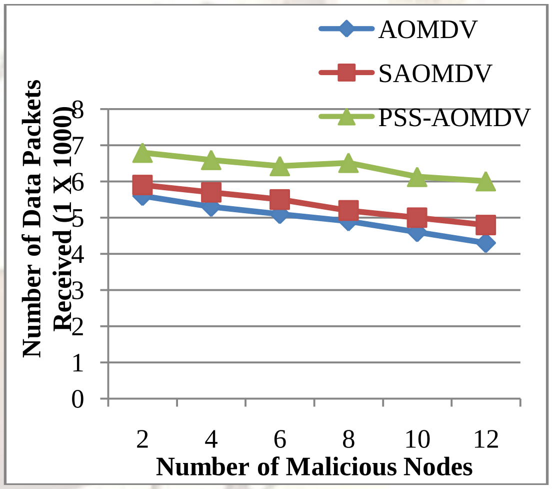

Figure 4.1: No. of Data Packets Vs No. of Malicious Nodes

4.2. Packet Delivery Ratio (PDR) Vs No. of Malicious Nodes

Packet Delivery Ratio (PDR) is the proportion of the amount of data packets received by the target node to the amount of data packets transmitted by the source node. It is clear from figure 4.2 that PDR of AOMDV and SAOMDV is significantly affected by the introduction malicious nodes whereas the PDR of PSS-AOMDV is not affected much when comparing with other two approaches.

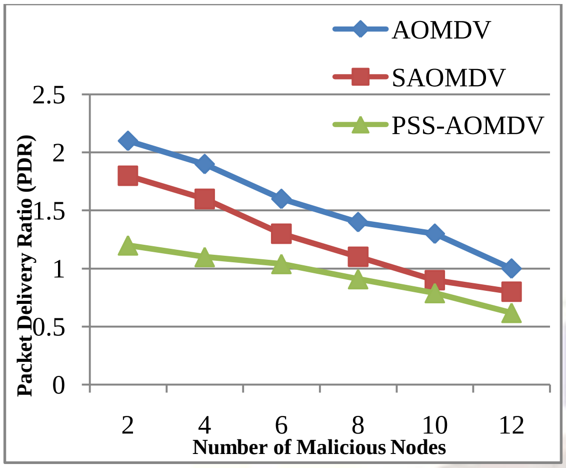

Figure 4.2: Packet Delivery Ratio (PDR) Vs No. of Malicious Nodes

V. Conclusion

MANET security is becoming a major concern and it is very vital in this present wireless environment. A secured routing protocol must provide security against the intruders and their attacks. The proposed routing protocol integrates the AOMDV with Proactive Bai's secret sharing scheme with the purpose of providing a secured communication in MANET. In this paper, a secured ad-hoc on-demand multipath distance vector routing protocol and it is named as PSS-AOMDV, since it uses Proactive Bai's secret sharing scheme. This scheme helps in easily recognizing the malicious nodes by providing proper authorization since only the users with proper key are permitted to share and reconstruct the secret.

In this scheme, the secret cannot be revealed by simply obtaining a mixture of k past shares and present shares. This scheme ensures the adversaries cannot obtain the projection matrix S when the shares are periodically renewed.

The simulation result confirms that PSS-AOMDV is less vulnerable to the intrusion of malicious nodes and moreover there is only lesser effect in the packet delivery ratio.

References

[1] Luo Junhai, Ye Danxia, Xue Liu, and Fan Mingyu, "A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks", IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, Pp. 78-91, 2009.

[2] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, "Survey of routing attacks in Mobile Ad-Hoc Networks", IEEE wireless communication, Pp. 85-91, 2007.

[3] Hongmei Deng, Wei Li, and Dharma P. Agarwal "Routing security in wireless Ad Hoc networks", IEEE Communications Magazine, 2002.

[4] M. Guerrero Zapata and N. Asokan, "Securing Ad hoc Routing Protocols," in Proceedings of the 1st ACM workshop on Wireless security, Atlanta, GA, USA, Sep 2002, pp. 1–10.

[5] Cerri, D. Ghioni, A. "Securing AODV: the A-SAODV secure routing prototype", IEEE Communications Magazine, Vol. 46, No. 2, page(s): 120 – 125, 2008.

[6] Li Bai, "A Strong Ramp Secret Sharing Scheme Using Matrix Projection", Proceedings of International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06), Pp. 656, 2006.

[7] R. Perlman, Fault-tolerant broadcast of routing information, Computer Networks, 7, 395–405 (1983).

[8] L. Zhou, and Z. J. Haas, Securing ad-hoc networks, IEEE Network Mag., 13, 24–30 (1999).

[9] Kotzanikolaou, P.; Mavropodi, R.; Douligeris, C.; "Secure Multipath Routing for Mobile Ad Hoc Networks", WONS 2005. Second Annual Conference on Wireless On-demand Network Systems and Services, Page(s): 89 – 96, 2005.

[10] Marina MK, Das SR, "Routing performance in the presence of unidirectional links in multihop wireless networks", In Proceedings of ACM MobiHoc, 2002.

[11] Nasipuri A, Castaneda R, Das SR, "Performance of multipath routing for on-demand protocols in mobile ad hoc networks", ACM/Kluwer Mobile Networks and Applications (MONET), Vol. 6, No. 4, Pp. 339–349, 2001.

[12] Adi Shamir, "How to Share a Secret", Communications of the ACM, Vol. 22, No. 11, Pp. 612-613, 1979.

[13] Marina MK, Das SR, "Performance of route caching strategies in dynamic source routing", In Proceedings of Workshop on Wireless Networks and Mobile Computing (WNMC) in conjunction with International Conference on Distributed Computing Systems (ICDCS), 2001.

[14] Perkins CE, Belding-Royer E, Das SR, "Ad hoc on-demand distance vector (AODV) routing", http://www.ietf.org/rfc/rfc3561.txt, 2003.

[15] Kumar, H.; Sarma, D.; Kar, A.; "Security threats in wireless sensor networks", IEEE Aerospace and Electronic Systems Magazine, Vol. 23, No. 6, Pp. 39 – 45, 2008.

[16] Herzberg A, Jarecki S, Krawczyk H and Yung M, "Proactive secret sharing or: how to cope with perpetual leakage", in Don Coppersmith (Ed.): Advances in Cryptology – Crypto '95, August, Santa Barbara, CA, Pp. 339–352, 1995.

[17] Li Bai and XuKai Zou, "A Proactive Secret Sharing Scheme in matrix projection method", Int. J. Security and Networks, Vol. 4, No. 4, Pp. 201-209, 2009.