ISSN 2229-5518

Bai's Secret Sharing Scheme for Highly Secured AOMDV Routing Protocol

C. Chandrasekar, *Lt.Dr. S. Santhosh* Baboo

Abstract--- Security in wireless network is of a great concern in the present wireless environment. Security is becoming a much essential part in wireless communication as intruders are very much keen in attacking the transmitted route or any node to steal the data packets It is indispensable to provide security to the network from the intruders and their security attacks. In order to provide a secured environment, it is essential that routing protocol exploited in a MANET should be of highly secured from the intruders. There are several routing protocols exist but most of these protocols makes use of only a single path. Therefore, proposed a Highly Secured Ad-hoc On-demand Multipath Distance Vector routing protocol (HSAOMDV) using the Bai's secret sharing scheme. Secret sharing scheme allows to distribute a secret only between a set of participants in a communication process by providing each participant a share. By this manner only the group of participants are allowed to reconstruct the secret. In order to evaluate the performance of the proposed HSAOMDV, it is compared against AOMDV and SAOMDV (AOMDV with Shamir's Secret Sharing Scheme). Number of packets received by HSAOMDV routing protocol does not decreased with intrusion of malicious nodes in the network and the packet delivery ratio also comparably high than the other two routing protocols.

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

I. INTRODUCTION

Mobile Ad-hoc NETwork (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.

C. Chandrasekar, Research Scholar , Computer Science, Manonmaniam Sundaranar University, Tirunelveli - 627 012, chandrasekar2000@gmail.com

Lt.Dr. S. Santhosh Baboo, Reader, P.G. and Research, Dept of Computer Science, D.G.Vaishnav College, Chennai – 600106.

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].

In this paper, Bai's secret sharing scheme is used for the purpose of providing better security among MANET nodes. 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. The main aim is to sustain the genuineness of the nodes available 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, Bai's secret sharing scheme is incorporated to AOMDV to make it as Highly Secured AOMDV (HSAOMDV). In HSAOMDV, only the authorized users are allowed to take part in the communication.

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 behaviour. 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 misbehaviour 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.

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 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 guarantee 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.

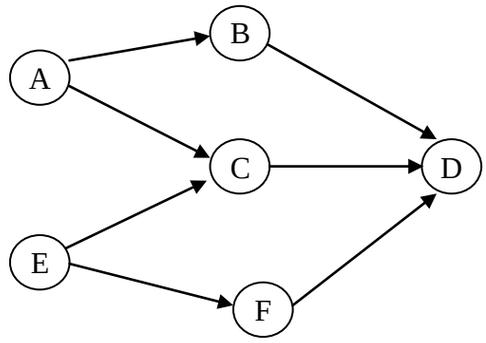

Figure 3.1: Paths maintained at different nodes to a destination possibly will not be equally disjoint.

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.

3.2. Secret Sharing in AOMDV

SAOMDV with Shamir's secret sharing scheme is described in short before introducing the Bai's secret sharing scheme using matrix projection.

SAOMDV with Shamir's Secret Sharing Scheme

Shamir [12] developed the scheme of a (k, n) threshold-dependent secret sharing scheme. This scheme permits a polynomial function of the $(k-1)$th power as,

$$f(x) = s + d_1x + d_2x^2 + \cdots + d_{k-1}x^{k-1} (\text{mod } p),$$

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

The polynomial function f(x) is destroyed after each shareholder possesses a pair of values (x_i, y_i) in order that no single shareholder recognizes the secret value s. No groups of $(k-1)$ or smaller amount secret shares can find out the secret s. Alternatively, when k or more secret shares are accessible, then might set up at least k linear equations $y_i = f(x_i)$ for the unidentified x_i's and s. The distinctive solution to these equations confirms that the secret value s can be easily acquired by means of Lagrange interpolation.

Major Disadvantages of using Shamir's Secret Sharing Scheme in AOMDV

- One of the major concerns of this scheme is that it has an extremely easy access structure. Any *k* out of *n* participants are capable of reconstructing the secret.
- An additional disadvantage of this scheme is that if the size of the share enlarges with the increase in the number of participants in a communication process, the size of the share also becomes larger.
- The most common disadvantage of this Shamir's secret sharing scheme is its complexity. In case

of exploiting a secret sharing scheme in a wireless networking environment, it must be noted that it should not generate intolerable delays.

3.3 Bai's Secret Sharing Scheme using Matrix Projection

In this section designed highly secured AOMDV with Bai's secret sharing scheme.

Consider A be an $m \times k$ matrix with rank $k(m \geq k > 0)$, and

$$S = A(A'A)^{-1}A',$$

where $(\cdot)'$ is the transpose of a matrix and $m \times m$ matrix S is A's projection matrix,

$$S = \text{proj}(A)$$

The vectors v_i using k can be calculated linearly independent $k \times 1$ vectors x_i,

$$v_i = Ax_i,$$

in which $1 \leq i \leq k$. These $m \times 1$ vectors v_i can be placed in

$$B = [v_1\ v_2 \ldots v_k].$$

Based on the Invariance Theorem [3], the projection matrix of B must be similar as that of A:

$$A(A'A)^{-1}A' = B(B'B)^{-1}B'$$

3.3.1. Steps in Bai's Secret Sharing Scheme

Following is the procedure used for the secret sharing in HSAOMDV.

Phase I : Construction of Shares

For a secret matrix S, the shares are generated as:

1. Create an $m \times k$ random matrix A of rank k in which $m > 2k - 3$,
2. Select n random $k \times 1$ vectors x_i (any k vectors are linearly independent),
3. Compute share $v_i = (A \times x_i)(\text{mod } p)$ for $1 \leq i \leq n$.
4. Calculate $S = \text{proj}(A)$,
   Calculate $R = (s - S)\ (\text{mod } p)$,
5. Destroy matrix A, x_is, and S and s.
6. Distribute n shares v_i and make R publicly known.

Phase II : Reconstruction of Secret

In order to reconstruct, the secret s with k or more shares v_i, the procedure is followed,

7. Collect shares $v_{i_1}\ v_{i_2} \ldots v_{i_k}$
8. Generate a matrix B using only k shares as $B = v_1\ v_2 \ldots v_k$.
9. Compute the projection matrix $S = \text{proj}(B)$,
10. Calculate $S = (S + R)\ (\text{mod } p)$.

It is to be observed that in step 1 of phase one, the constraint that $m > 2k - 3$ comes from a condition to appropriately apply matrix projection technique to multiple secret sharing.

In steps 2 and 3 of phase two, once the groups of participants have calculated B and S, they must make sure whether B has a rank k. If any of these steps fail to satisfy, it is identified that there must be some unintentional errors or dishonest behavior or intruders attack. By this manner, this scheme also becomes partially verifiable.

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 meter2
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	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 HSAOMDV remains almost steady. It indicates that malicious nodes have only lesser consequence on the amount of data packets transmitted by HSAOMDV. Simultaneously, the data packets received in AOMDV and SAOMDV falls considerably with the increase in the number of malicious nodes.

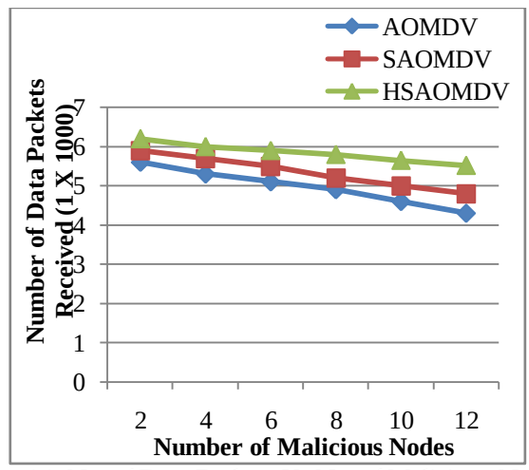

Figure 4.1: No. of Data Packets Vs No. of Malicious Nodes

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 while the PDR of HSAOMDV is unaffected to it.

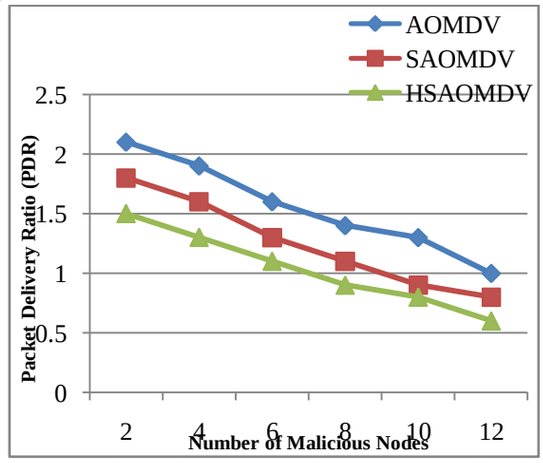

Figure 4.2: Packet Delivery Ratio (PDR) Vs No. of Malicious Nodes

V. CONCLUSION

Security of MANET is becoming a major concern and it is turning out to be an essential research in the field of wireless networks. A highly secured routing protocol must provide security against the intruders and the attacks. The proposed routing protocol combines the AOMDV with Bai's secret sharing scheme with the purpose of providing a secured communication. In this paper, a highly secured ad-hoc on-demand multipath distance vector routing protocol called HSAOMDV. This scheme helps in easily recognizing the malicious nodes by providing proper authorization since only the users with proper key are allowed to share and reconstruct the secret. The simulation result confirms that HSAOMDV is less vulnerable to the intrusion of malicious nodes and moreover there is no 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.