An Efficient and Secured AOMDV Routing Protocol with Shamir's Secret Sharing Scheme

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

C. Chandrasekar
Research Scholar
Computer Science
Manonmaniam Sundaranar University
Tirunelveli - 627 012

ABSTRACT
Security has turned out to be a most important concern to facilitate secured communication between mobile nodes in a wireless environment. It is essential to protect the network from several kinds of security attacks. Recently, large numbers of routing protocols have been developed. But, most of the available protocols are single path or makes use of only a certain path at a particular time or can not prevent both the passive attacks and active attacks at the same time. Hence, propose a secured Ad-hoc On-demand Distance Vector routing protocol (AOMDV) based on secret sharing. Cryptography is one of the efficient technique to provide security to data being broadcasted in wireless communications systems. Enhanced information security can be offered by integrating AOMDV and Shamir's secret sharing scheme. In this approach, keys are produced by source and transmitted to the other nodes in the network. AOMDV and SAOMDV (AOMDV with Shamir's Secret Sharing Scheme) are simulated and the performance of both the protocols are evaluated. The performance of Secured AOMDV was stable but that of AOMDV was found to be degrading sharply with intrusion of malicious nodes in the network.

Keywords
Mobile Ad Hoc Networks, Multihop Wireless Networks, On-Demand Routing, Multipath Routing, Secret Sharing

1. INTRODUCTION
A mobile ad hoc network is a mobile, multihop wireless network that does not depend on any predefined infrastructure. Mobile ad hoc networks (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.

The security in MANETs 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 function of 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.

In this paper, Shamir secret sharing approach 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. In this secret sharing approach, a key is transmitted or shared among the multiple individuals in the network that are under the procedure of encryption and decryption. The main aim is to sustain the genuineness of the nodes available in the network.

AOMDV is one of the potential protocols for maintaining security. It is found that total belief of the network on nodes can result in various routing attacks. In order to eliminate this problem, Shamir secret sharing is incorporated to AOMDV to make it Secured AOMDV (hence forth called SAOMDV). In SAOMDV, each node ensures the security of its neighbors before forwarding route requests. The route request packets are not given to malevolent nodes. This evaluation clearly, guarantees that malevolent nodes will not take part in the data transfer from the source to the destination.

2. LITERATURE SURVEY
The growth and development of telecommunication has increased the need for mobility, wireless or mobile networks and this desire has already swapped the wired networks. The upcoming networks

has entirely different infrastructure and has various protocols and devices. The main aim of this approach is to assess the two secure routing protocols Ariadne and SAODV in the performance characteristics rather than security features under random way point and Manhattan grid mobility models. Naeem et al., [6] used and implement the extension of AODV that is Secure Ad-hoc On-demand Distance Vector routing protocol (SAODV) and the extension of DSR that is Ariadne in the network simulator 2 (NS-2). In this paper, these protocols are compared with the quality of service parameters like delay, jitter, routing overhead, route acquisition time, throughput, hop count, packet delivery ratio using Manhattan grid and random waypoint mobility models. This paper mainly focuses on finding out the payload a node has to pay to assure the good quality of service.

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., [7] 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. 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.

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., [8] 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.

Perlman proposed a link state routing protocol [9] 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 [10] 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.

3. METHODOLOGY

3.1 Ad hoc On-Demand Distance Vector Routing

AODV [11, 12] is an on-demand, which follows single path, loop-free distance vector protocol. It incorporates the on-demand route discovery approach in DSR [13] with the notion of destination series numbers from DSDV [6]. But, different from DSR which employs source routing, AODV obtains a hop-by-hop routing method.

AODV [1] protocol is demonstrated to be a proficient routing protocol for implementation in Ad hoc networks. It is a Source-Initiated On-Demand or Reactive Routing Protocol. When a source node needs to send a message to a definite destination node to which it does not have a suitable route, it begins a route discovery process. The source node transmits a Route REQuest (RREQ) message to its neighbor nodes, which then promote the request to its neighbor nodes, and so on, with the anticipation of either the destination or an intermediary node with a route to the target in its routing table is attained. All through the process of forwarding the RREQ, an intermediary node record in its routing table (i.e., precursor list) the address of the neighbor from which the primary copy of the transmitting packet is received, thus setting up a reverse path. Supplementary copies of the similar RREQ received later are not considered. Once the RREQ arrives at the destination or an intermediary node with a route, the particular node responds by unicasting an RREP (Route REPly) message back to the neighbor from which it initially received the RREQ, which relays the RREP backward using the precursor nodes to the source node.

3.2 Ad hoc On-Demand Multipath Distance Vector Routing

The main objective of this paper is to provide a secured AOMDV routing protocol by means of incorporating Shamir's Secret Sharing scheme. In this section the goal is to enhance the AODV 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 [14].

3.3 Protocol Overview

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 [15].

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.

3.4 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.

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.

3.5 Secret Sharing in AOMDV

The security of MANETs is commonly predicated on the accessibility of well-organized key management approaches. On the other hand,

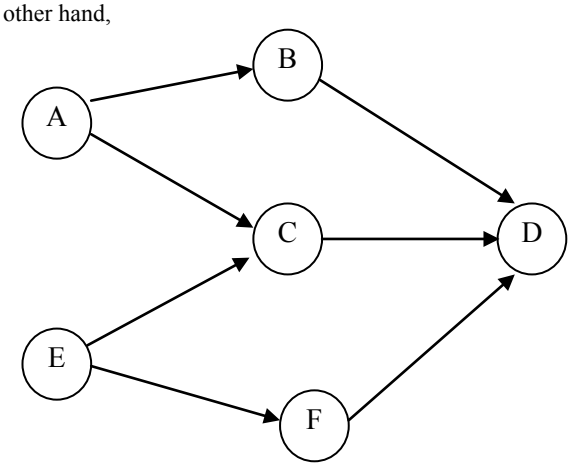

Figure 3.1: Paths maintained at different nodes to a destination possibly will not be equally disjoint.

centralized authority and (ii) dynamic behavior of MANETs, characterizes the chief obstacle in offering protected, efficient and competent key management technique. An additional complication is that the cryptographic keys should be established before the communication begins. Therefore, standard key exchange techniques, e.g., Station-to-Station protocol [16], are not suitable because: (i) they need the nodes to work together and (ii) they dependent on certain form of a Public Key Infrastructure (PKI) which is not generally offered in MANETs. In accordance with the latter is the fundamental use of public key cryptography which is extremely costly for some mobile devices.

Based on the problems discussed above, proposed an SAOMDV routing protocol in this paper by using secret sharing to solve these obstacles. In route request stage, this approach makes use of a cryptographic technique to design SAOMDV routing protocol, only the target node can recognize the identity of all nodes which involves in the communication and the route information. Furthermore, the key shared among the source and destination nodes is revealed following the route request stage. In route reply and data transmission stage, only the authorized nodes can acquire the functional information of paths while malevolent node acquires nothing. Shamir's secret sharing on the data transmission method is introduced and utilizes concurrent multipath routes to broadcast information, as a result it is complicated for attackers to analyze the routing information and traffic pattern.

3.6 Shamir's Secret Sharing Scheme

In certain cryptographic circumstance, it is essential to share a secret among the d nodes without any $k < d$ nodes being competent to recover the data packets transmitted. In [17] Shamir illustrates the difficulty and provided a secret sharing scheme by means of polynomial interpolation as a recovery purpose. Specifically, every node has a pair $(x_i, P(x_i))_{x_i \neq 0}$ where P is a polynomial of degree k, and the secret is specified by $P(0)$. In this pattern, one requires at least $k+1$ shares to recover P, then $P(0)$. The sharing and reconstruction algorithms for a value of $k = d - 1$, operating on n-bits words. With these constraints, with the intention of sharing a secret a_0 into d shares, one requires to select $d-1$ random numbers $(a_{d-1}, \dots, a_1)$to build the polynomial.

$$P(x) = a_{d-1} \cdot x^{d-1} + a_{d-2} \cdot x^{d-2} + \cdots + a_1 \cdot x + a_0$$

Every share i is then specified by (x_i, y_i) where $y_i = P(x_i)$, and the x_i 's are all different and non-zero. The algorithm used is given below.

Algorithm Shamir's Secret Sharing scheme

Input: A secret a_0, random values $(x_i)_{i=0\dots d-1}$
Output: Shares $(x_i, y_i)_{i=0\dots d-1}$

1. $(a_i)_{i=0\dots d-1} \leftarrow \boldsymbol{Rand}(n)$
2. **for** $i = 0$ to d **do**
3. $y_i \leftarrow a_{d-1} \cdot x_i^{d-1} + a_{d-2} \cdot x_i^{d-2} + \cdots + a_1 \cdot x_i + a_0$
4. **return** $(x_i, y_i)_{i=0\dots d-1}$

The reconstruction stage is directly obtained from the polynomial interpolation and progresses as follows:

$$a_0 = \sum_{0}^{d} y_i \cdot \beta_i$$

where each β_i is a previously calculated value such that

$$\beta_i = \prod_{j=0, j \neq i}^{d} \frac{-x_j}{x_i - x_j}.$$

4. EXPERIMENTAL RESULTS

A simulation testbed for mobile ad hoc network is built up to compare the performance of the AOMDV and SAOMDV routing protocol. Both these protocols were experimented over this testbed and its performance was evaluated for different circumstances.

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

It may be seen from Figure 4.1 that with the increase in the quantity of malicious nodes, the number of data packets transmitted by AOMDV increases slightly, while those by SAOMDV remains almost steady. It specifies that malicious nodes have no consequence on the amount of data packets transmitted by SAOMDV. At the same time as the data packets received in AOMDV falls significantly with increase in the amount of malicious nodes. At the beginning, packet received by the proposed SAOMDV increases gradually and then continues to be steady. It undoubtedly reveals that AOMDV is poorly affected by effect of malicious nodes but not in the case of SAOMDV.

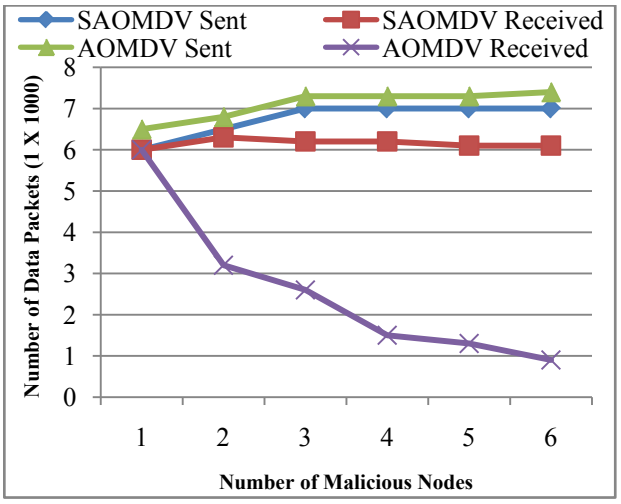

Figure 4.1: No. of Data Packets Vs No. of Malicious Nodes

4.2 Packet Delivery Ratio (PDR) Vs No. of malicious nodes

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 obvious from Figure 4.2 that PDR of AOMDV is greatly affected by the introduction malicious nodes while the PDR of SAOMDV is unaffected to it.

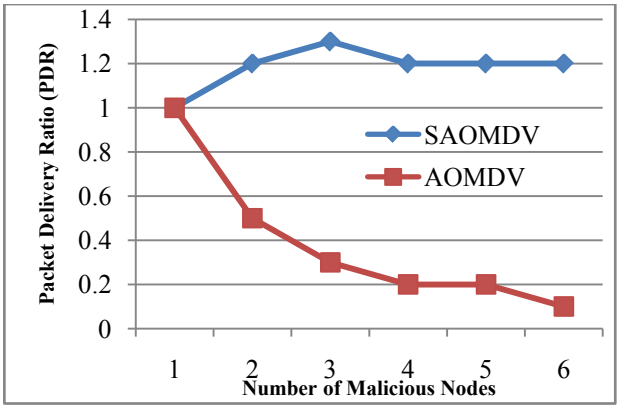

Figure 4.2: Packet Delivery Ratio (PDR) Vs No. of Malicious Nodes

5. CONCLUSION

In this paper, the security of MANETs against attacks like wormhole, blackhole etc, is concerned and a secured routing protocol is proposed successfully. The proposed routing protocol integrates the AOMDV with the Shamir's Secret Sharing scheme in order to provide a secure routing. In this paper, a secured on-demand multipath protocol called SAOMDV that extends the single routing path of AODV protocol to offer multiple paths for a single transmission and with the intention of enhancing the security Shamir's Secret Sharing scheme is integrated with AOMDV. With this proposed scheme it is simple for the source node to recognize the malevolent node that comes into the network without authorization. The simulation result reveals that SAOMDV is less prone to the attack of malicious nodes and there is no effect in the packet delivery ratio with the introduction of malicious nodes. Thus the result confirms that SAOMDV is more secured than the existing AOMDV.

6. 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] C. E. Perkin, E. M. Royer, "Ad-hoc on demand distance vector(AODV)routing", The Second IEEE Workshop on Mobile Computing Systems and Applications, 1999.

[6] Naeem, M.; Ahmed, Z.; Mahmood, R.; Azad, M.A.; "QOS based performance evaluation of secure on-Demand routing protocols for MANET's", International Conference on Wireless Communication and Sensor Computing, 2010, pages 1-6, ICWCSC 2010.

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

[8] 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.

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

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

[11] Perkins CE, Royer EM, "Ad hoc on-demand distance vector routing", In Proceedings of IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), 1999.

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

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

[15] 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.

[16] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and Its Applications, ISBN 0-8493-8523-7, 1997.

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