International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-3, Issue-2, March 2015

# Randomize Dissemination Path for Secure Data Transmission in Mobile Ad-Hoc Network

**Mr. Arvind P. Pande, Mr. B.S Patil , Mr. A. U Patil**

*Abstract—*

**Mobile ad hoc network (MANET) is an autonomous system of mobile nodes. The nodes are free to move arbitrarily. Due to lack of a centralized secure infrastructure, the communication is prone to security attacks and the nodes can be easily compromised. Security has become one of the major issues for data communication over wired and wireless networks so various security-enhanced measures have been proposed to improve the security of data transmission over public networks. The objective of proposed work is to improve routing security we propose a proactive mechanism as Randomized routing that explores the existence of multiple routes and forces packets to take alternate paths randomly from its neighbors that is a Randomize delivery path for secure data transmission. We maintain neighboring nodes of each node by sending hello packets. Then we find out delivery path from neighboring nodes by random operation excluding previous hop which is maintained as history node. Protocol RDSDV is implemented to randomize delivery paths and compared the proactive routing protocols DSDV and RDSDV for different number of nodes. The performance of these protocols is measured under a Particular scenario on the basis of three metrics as Packet delivery ratio, e2e delay and jitter.**

***Index Terms*: JITTER, MANET, PDR, R-DSDV, NS2, XGraph**

## I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre- existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. The topology of such networks is likely highly dynamic because each network node can freely move and no pre-installed base stations exist. Due to the limited wireless transmission range of each node, data packets then may be forwarded along multi hops.

**Manuscript received March 10,2015**

**Mr. Arvind P. Pande,** Department of Information Technology, Shivaji University, Sangli, Maharashtra India,
**Mr. B. S Patil**, Department of Information Technology, Shivaji University, Sangli, Maharashtra India
**Mr. A. U Patil**, Department of Information Technology, Shivaji University, Sangli, Maharashtra India

Security problems in MANET in term of authentication have been studied extensively in over two decades. First the threshold cryptography proved to be an effective scheme for key management and distribution. However it adds overhead to routing and increases traffic in the network. The attacks such as wormhole and Denial of Service (DoS) [9] can compromise routes through spoofing ARP or IP packets, passively or actively. Due to bandwidth constraints and energy conservation, an efficient implementation of the scheme is critical. Existing work on security-enhanced data transmission [3] includes the designs of cryptography algorithms and system infrastructures and security- enhanced routing methods. Their common objectives are often to defeat various threats over the Internet, including eavesdropping, spoofing, session hijacking, etc.

Among many well-known designs for cryptography based systems, the IP Security (IPSec) and the Secure Socket Layer are popularly supported and implemented in many systems and platforms. Although IPSec and SSL do greatly improve the security level for data transmission, but they introduce substantial overheads which is unavoidable. Especially on gateway/host performance and effective network bandwidth. For example, the data transmission overhead is 5 cycles/byte over an Intel Pentium II with the Linux IP stack alone, and the overhead increases to 58cycles/byte when Advanced Encryption Standard (AES) is adopted for encryption/decryption. Different from the past work on the designs of cryptography algorithms and system infrastructures, we designed a Randomize delivery paths algorithm for data transmission in mobile ad hoc network..

## II. SECURITY ISSUES

The security of communication in ad hoc wireless networks is important, especially in military applications. The absence of any central coordination mechanism and shared wireless medium makes MANETs more vulnerable to digital/cyber-attacks than wired networks. These attacks are generally classified into two types: passive and active attacks. Passive attacks do not influence the functionality of a connection. An adversary aims to interfere in a network and read the transmitted information without changing it. If it is also possible for the adversary to interpret the captured data, the requirement of confidentiality is violated. It's difficult to recognize passive attacks because under such attacks the network operates normally. In general, encryption is used to combat such attacks.

Active attacks aim to change or destroy the data of a transmission or attempt to influence the normal functioning of the network. Active attacks when performed from foreign networks are referred to as external attacks. If nodes from within the ad-hoc network are involved, the attacks are referred to as internal attacks. This protocol is implemented to combat passive and active attacks.

## III. SCOPE OF SECURITY

Security in mobile ad hoc networks is very important because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, the absence of certification authority, and the lack of a centralized monitoring or management point. To protect information and resources from attacks and misbehavior. The requirements that effective security architecture must ensure Availability, Authentication, Data confidentiality, Integrity & non rejection.

Systems that ensure availability in MANETs seek to combat denial of service and energy starvation attacks, as well as node misbehavior such as node selfishness in packet forwarding. The core functionalities provided are routing and packet forwarding, and are closely related. The data Forwarding service consists of correctly relaying the received packets from node to node until they reach their final destination, the routes selected and maintained by the routing protocol.

These features can be exploited by malicious nodes to eavesdropping packets in transit, and then analyze them to obtain confidential and sensitive information. The preventive solution to protect information is to encrypt packets, but data encryption does not prevent malicious nodes from eavesdropping and trying to break decryption keys. Since packets follow multi-hop routes and pass through mobile nodes, a malicious node can participate in routing, include itself in routes, and drop all packets it gets to forward. Malicious attacks or selfish misbehavior on either of them will disrupt the normal network operations.

This protocol is designed mainly to overcome security attacks such as DoS, resource consumption attack and dropping data packets attack caused by malicious nodes. In Proposed algorithm, for data delivery of a packet with the destination at a node, to minimize the probability that packets are eavesdropped over a specific link, a randomization process for packet deliveries. In this process, the previous next-hop for the source node s is identified in the first step of the process. Then, the process randomly picks up a neighboring node as the next hop for the current packet transmission. The exclusion for the next hop selection avoids transmitting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

## IV. RANDOMIZED-DSDV

A Destination-Sequenced Distance Vector (DSDV) routing protocol is a typical routing protocol for MANETs, which is based on the Distributed Bellman-Ford algorithm [3]. In DSDV, each route is tagged with a sequence number which is originated by destination, indicating how old the route is [2]. All nodes try to find all paths to possible destinations nodes in a network and the number of hops to each destination and save them in their routing tables. New route broadcasts contain the address of destination, the number of hops to reach the destination, the sequence number of the information receive regarding the destination, as well as a new unique sequence number for the new route broadcast [2].

The delivery of a packet with the destination at a node. In order to minimize the probability that packets are eavesdropped over a specific link, a randomization process for packet deliveries, in this process, the previous next-hop for the source node is identified in the first step of the process. Then, the process randomly picks up a neighboring node as the next hop for the current packet transmission. The exclusion for the next hop selection avoids transmitting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

## V. IMPLEMENTATION

This protocol is implemented using network simulator 2 tool. NS2 is a discrete event simulator targeted at networking research and is widely utilized among academic researchers. It is an object oriented open source simulator written in OTcl and C++ [1] [2] NS2 provides substantial support for simulations of TCP, UDP, IP routing, and multicast protocols over wired and wireless networks, and it is supported by several research organizations. It helps to debug problems in a controlled environment. NS2 also helps in performing Analysis of hypothetical changes. Because it is open source, new functions and new algorithms can be added by modifying the source files. We implemented the new routing protocol as R-DSDV by modifying codes from DSDV source code

in NS2. This is implemented partly in OTcl and partly in C++. We designed RDSDV_PACKET as a new packet structure to find out neighboring nodes. The neighboring nodes are maintained with routing table at each node. Packet forwarding is done by selecting a random node from neighboring list excluding previous node which delivered a packet. This protocol is tested on simulation of different topologies with different numbers of nodes. The results are obtained from trace files by writing awk script for different performance metrics. These results are obtained for DSDV and R-DSDV protocols and plotted Graphs by xgraph tool. Following table shows network simulation parameters which are configured in tcl script as network interface, queue type and simulation area and others.

Table 6.1 Network Simulation Parameter

| Parameters | Values |
|---|---|
| Network interface/channel type | Wireless |
| Radio-propagation model | TwoRayGround |
| Network interface type | Phy/WirelessPhy |
| packet size | 512bytes |
| Interface queue type | Queue/DropTail/PriQueue |
| Max packet in IFQ | 50 |
| Number of mobile Nodes | 50 |
| Simulation area size | 1000*1000 |
| Simulation duration | 150 second |
| Transmission range | 250 m |
| Mobility model | Random |
| Routing protocols | RDSDV ,DSDV |

## VI. PERFORMANCE EVALUATION

To compare the performance of the two protocols under different scenario. In comparing the two protocols, the evaluation could be done in the following three metrics:

### *A. Packet Delivery Ratio:*

The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. PDR =∑ Number of packet receive / ∑ Number of packet send. The greater value of packet delivery ratio means the better performance of the protocol.

### *B. End to End Delay:*

The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. End to End Delay = ∑ (arrive time – send time) / ∑ Number of nodes.

### *C. Jitter:*

It is an important parameter for evaluating the performance of this protocol. Here it means the time difference between deliveries of two consecutive packets to the destination. Our aim is two randomize the delivery paths, so every packet takes different path to reach destination.

average jitter= ∑ [((recvtime(j)-sendtime(j))-(recvtime(i)-sendtime(i)))/(j-i)]/ number of nodes

Because of path variation, jitter value is larger for this protocol as compared DSDV protocol and as increases as number of nodes increases. We find out experimental results on above performance metric in following scenario as we consider node mobility speed30 m/s and size 1000 X 1000 m. Topology Size Width: 1000 Height: 1000.

Table 2. Jitter value variation

| Nodes | Jitter of DSDV | Jitter of RDSDV |
|---|---|---|
| 30 | 0.002867 | 0.002997 |
| 50 | 0.002820 | 0.003928 |
| 70 | 0.002720 | 0.004069 |
| 90 | 0.003141 | 0.003969 |
| 110 | 0.003462 | 0.0168 |

Table 2 show that, the jitter value is greater for randomized DSDV protocol as compared to DSDV protocol for topologies with different number of nodes.

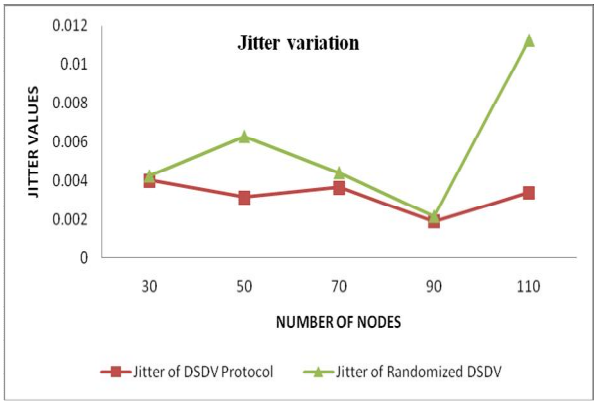


Fig.1: Jitter Variation

Figure 1 shows that , Jitter value is less in case of DSDV protocol because it uses shortest path routing algorithm so probability of delivery path following by two consecutive packets are same. So average jitter values is less as compared to our RDSDV(Randomized DSDV) protocol.
In case of RDSDV protocol, each packet is delivered on different path so time required for packet delivery is different which results jitter value for RDSDV is greater than DSDV protocol.

Table 2. PDR & EEDELAY value variation

| PDR & END TO END DELAY VARIATION | | | | |
|---|---|---|---|---|
| Nodes | PDR (%) | | End to End Delay | |
| | DSDV | R-DSDV | DSDV | R-DSDV |
| **30** | 98.82 | 99.39 | 135.63 | 126.81 |
| **50** | 99.47 | 98.17 | 139.88 | 136.11 |
| **70** | 99.91 | 99.91 | 142.16 | 139.33 |
| **90** | 97.10 | 96.12 | 159.18 | 166.54 |
| **110** | 91.90 | 88.84 | 208.52 | 211.68 |

Table 2 shows that, the PDR value & End to End Delay values are near about same for Randomized DSDV protocol as compared to DSDV protocol for topologies with different number of nodes.

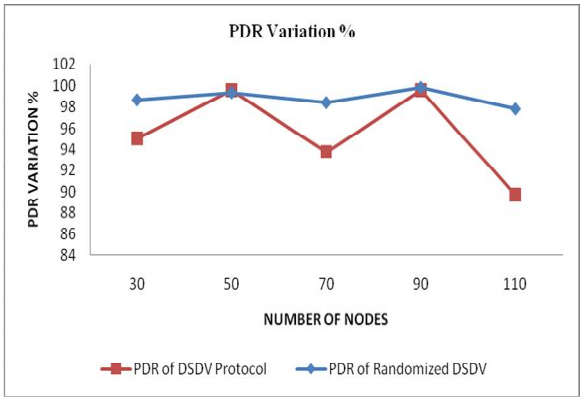


Fig 2: PDR variation

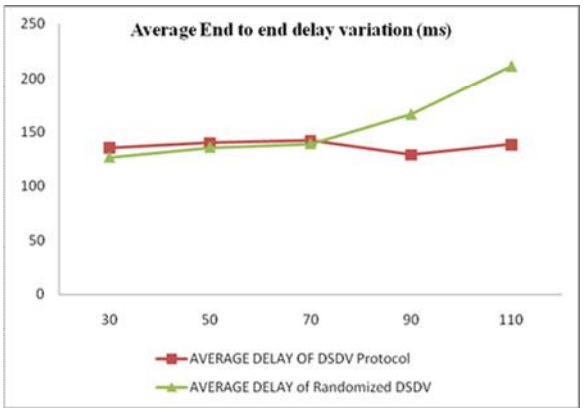


Fig.3: Average end to end delay variation

From table 2 we plotted graph to compare the performance of DSDV & R-DSDV protocol. Figure 2 & 3 shows that, PDR (Packet Delivery Ratio) value and End to End Delay values are very close for DSDV protocol and R-DSDV protocol.

This shows that overall performance in terms of packet delivery ratio is better than DSDV protocol and average end to end delay is almost same for nodes below 90.for node number above 90, it is better than DSDV protocol.

## VII CONCLUSION

To protect information and resources from active, passive attacks and misbehavior. We implemented randomized delivery path protocol. In order to minimize the probability that packets are eavesdropped over a specific link, we implemented a randomization process for packet deliveries. In this process, randomly picks up a neighboring node as the next hop for the current packet transmission. The exclusion for the next hop selection avoids transmitting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

Experimental results shows that jitter value is greater and increases as number of nodes increases hence prove that each packet transmitted at different path to destination. The PDR and End to End Delay metrics of R-DSDV protocol are closer to the metrics for DSDV protocol under same topology. We conclude that security attacks can be avoided by this process without reducing performance.

## VIII. REFERENCES

[1] Loay Abusalah , 2008 "A Survey of Secure Mobile Ad Hoc Routing Protocols," IEEE communications surveys vol. 10, no. 4
[2] Secured-destination Sequenced Distance Vector (SSDV) November 2011 International Journal of Computer Science and Telecommunications.
[3] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha, 2000 "Securing Electronic Commerce: Reducing the SSL Overhead," IEEE Network,.
[4] S. Bohacek, J.P. Hespanha, K. Obraczka, J. Lee, and C. Lim, 2002 "Enhancing Security via Stochastic Routing," ICCCN
[5] P. Papadimitratos and Z.J. Haas, 2002 "Secure Routing for Mobile Ad Hoc Networks," in SCS Communication Networks and Distributed Systems
[6] R. Stone, "CenterTrack: An IP overlay network for tracking DoS floods," in 9th USENIX Security Symposium, 2000.
[7] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in Proceedings of the 2000 ACM SIGCOMM Conference, (Stockholm, Sweden), pp.295–306, August, 2000.
[8] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, and R. Morris, "Resilient overlay networks," in Proc. 18th ACM SOSP, (Banff, Canada),2001.
[9] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for Web transactions," ACM Trans. on Information and System Security, vol. 1, pp. 66–92,1998.
[10] J. P. Hespanha and S. Bohacek, "Preliminary results in routing games," in Proc. Of the 2001 American Control Conference, June, 2001.
[11] [11] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, and R. Morris, "Resilient overlay networks," in Proc. 18th ACM SOSP, (Banff, Canada),2001.
[12] M. K. Reiter andA. D. Rubin, "Crowds: AnonymityforWeb transactions," ACM Trans. on Information and System Security, vol. 1, pp. 66–92, 1998.
[13] [13] J. P. Hespanha and S. Bohacek, "Preliminary results in routing games," in Proc. Of the 2001 American Control Conference, June, 2001.
[14] S. D. Patek and D. P. Bertsekas, "Stochastic shortest path games," SIAM J Contr. Optimization, vol. 37, pp. 803–824, 1999.
[15] The VINT Project, a collaboration between UC Berkeley, LBL, USC/ISI and Xerox PARC, "The ns manual (formerly ns Notes and Documentation)." http://www.isi.edu/nsnam/ns/ns-documentation.html, Oct. 2000.
[16] K. Sollins, "The TFTP protocol." RFC 1350, 1992.
[17] Wenjing Lou and YuguangFang , "AMultipath Routing Approach for SecureData Delivery", IEEE Conference, 2001,pp.1467-1473

**Mr. Arvind P Pande** : Master of Engineering in Electronics , Microsoft certified Technology Specialist. Working as assistant professor in Information Technology department. Total 12 Years of Experience in Networking, MANET,WSN and Image Processing.

**Mr. B. S Patil** Master of engineering in Electronics Working as associate professor in Electronics department. Total 23 Years of Experience in Networking and Video engineering.

**Mr. A. U Patil** pursing Master of engineering in Computer Science. Working as assistant professor in Information Technology department. Total 4 Years of Experience in Networking, and cloud computing.