International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 7, July - 2013

# Secure Routing Schema For Safeguarding Communication System In MANET

Najiya Sultana
*Research Scholar*.
Janardan Rai Nagar Rajasthan Vidyapeeth University
Udaipur, India

Prof. Shiv Singh Sarangdevot
*Vice Chancellor*
Janardan Rai Nagar Rajasthan Vidyapeeth University
Udaipur, India

***Abstract*— With the faster pace of modern communication system, mobile adhoc network (MANET) has played a crucial role for mechanizing packet forwarding in wireless networking system. With absence of any types of infrastructure, mobile nodes participate in data packet forwarding using intermediary peers. Due to inherent charecteristics of MANET, security loopholes and threats have posed an exponential challenge in routing protocols. Various types of lethal attacks in MANET usually targets data, bandwidth, battery etc. Therefore, the present paper proposes a secure mechanism using hop-by-hop packet forwarding that governs the routing schema. Experimented over platform independent source, the proposed algorithm shows maximum reliable data transmission using secure hop-by-hop routing schema with highest score of packet delivery ratio.**

***Keywords-component:*** Routing, MANET, security

## I. INTRODUCTION

Mobile Ad hoc Network (MANET) is self-configuring infrastructureless network of mobile devices connected by wireless. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features [1] Unreliability of wireless links between nodes, constantly changing topology, and lack of incorporation of security features. According to security information with respect to MANET network are vulnerable compromises or physical capture, especially at the end of low-end devices due to weak protection. Intruders enter into the network and poses weakest link and incur a domino effect of security in the network. According to wireless channel is concerned bandwidth is one of constrained and use to share among multiple different network nodes. There is also one more restriction that is computation capability; like low-end devices for e.g. PDAs, can hardly perform low computation due to this way they usually use asymmetric cryptographic computation which is bit low complex, because mobile devices have very limited energy resources due to this way mostly mobile devices powered by batteries. The wireless medium as compared to wireline network node mobility more dynamics in mobile adhoc networks. The network topology is highly dynamic due to free movement in the network like nodes can frequently join or leave, as well as in the network by their own will. There are also interferences in the wireless channel due to this way error, exhibiting volatile characteristics in terms of bandwidth and delay occurs. Due to such dynamic behaviors mobile users request for security services at any anytime or anywhere whenever they move from one place to another in the network. Among all these security services, authentication is probably the most important and complex issue in MANETs because it is the bootstrap of the whole security system. Once authentication is achieved in MANET then confidentiality is just a matter of encrypting algorithm on the session by using keys. These security services can be provided singly or in combination, it only depends on our requirements. It is also true that security has long been an active research topic in wireline networks; but due to unique characteristics of MANET there are many challenges because of its self organizing behavior. These challenges are shared wireless medium, highly dynamic network topology, stringent resource constraints and open network architecture. It's true that existing security solutions for wired networks do not directly apply to the Mobile ad hoc networks domain. The proposed system will introduce a new scheme of secure routing scheme from hop-to-hop in less network overhead and more secure way. Section 2 discusses about the related work followed by problem description in section 3. Proposed system is discussed in section 4 followed by algorithm execution and results in Section 5 along with conclusion in Section 6.



## II. RELATED WORK

Yadav et al. [2] have introduced in this paper on demand routing protocols AODV, DSR and DYMO based on IEEE 802.11 are examined and characteristic summary of these routing protocols is presented. Parma Nand et al. [3] has introduced in this paper on demand routing protocols AODV, DSR and DYMO. Johnson et al. [4] has presents a protocol for routing in ad hoc networks that uses dynamic source routing. Lin et al. [5] have presented a novel anonymous secure routing protocol for mobile ad hoc networks (MANETs). Su et al. [6] has proposed mechanisms to complement the existing secure routing protocols to resist the creation of in-band tunnels. Jaafar et al. [7] they introduced some evaluation and performance comparisons of AODV, SAODV and A-SAODV routing protocols in MANETs. Singh et al. [8] has introduced in this paper, various existing routing protocols were reviewed. Francq et al. [9] has proposed countermeasure

provides a high level of fault detection. Defrawy et al. [10] has presents the PRISM protocol which supports anonymous reactive routing in MANETs. Kurosawa et al. [11] has proposed an anomaly detection scheme using dynamic training method. Thakare et al. [12] has introduced in this paper, an attempt has been made to compare the performance of two prominent on demand reactive routing protocols for MANETs. Sanzgiri et al. [13] has proposed propose a solution to one, the managed-open scenario where no network infrastructure is pre-deployed. Crrepeau et al. [14] they were presented Robust Source Routing (RSR). Qabajeh et al. [15] has proposed a new model of routing protocol called ARANz, which is an extension of the original Authenticated Routing for Ad-Hoc Networks. Feng He et al. [16] have proposed a novel secure routing protocol S-MAODV which is based on MAODV. Mondal et al. [17] has presented the analytical results for the probability of success of data transmission over the networks taking the probability of success or failure of individual paths different.

## III. Problem Description

The delay inherent property of Mobile Adhoc Network is characterized by a very sparse node population and by the lack of full network connectivity at virtually every time. Given these features, eventual packet delivery to the destination can be achieved only through node mobility, which is indeed the main communication means in the network.

- Each node may act not only as a relay carrying and forwarding messages for other nodes, but also as a source trying to deliver out its locally generated message.
- Thus, a node may become more willing to forward its own message rather than that of others when it encounters some node.
- This kind of selfish behaviors may become much more significant when the nodes are operating under both QoS requirements (e.g., delivery delay requirements) and energy consumption constraints.
- These kinds of node selfishness in relay cooperation and analytically explore how it will influence the delivery performance of the two-hop relay routing in the challenging MANET networks.

MANET maximizes cumulative network throughput by using all available nodes for routing and forwarding. Therefore, the more nodes that participate in packet routing, the greater the aggregate bandwidth, the shorter the possible routing paths, and the smaller the possibility of a network partition. However, a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious, or broken. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets. A selfish node is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. A malicious node launches a denial of service attack by dropping packets. A broken node might have a software fault that prevents it from forwarding packets.i have a software fault.

## IV. Proposed System

This prime aim of the work is to establish the fundamentals to implement in the future security so that mobile adhoc protocol can also thwart various attacks, which could be launched by certain malicious nodes that originate due to routing issue in MANET.

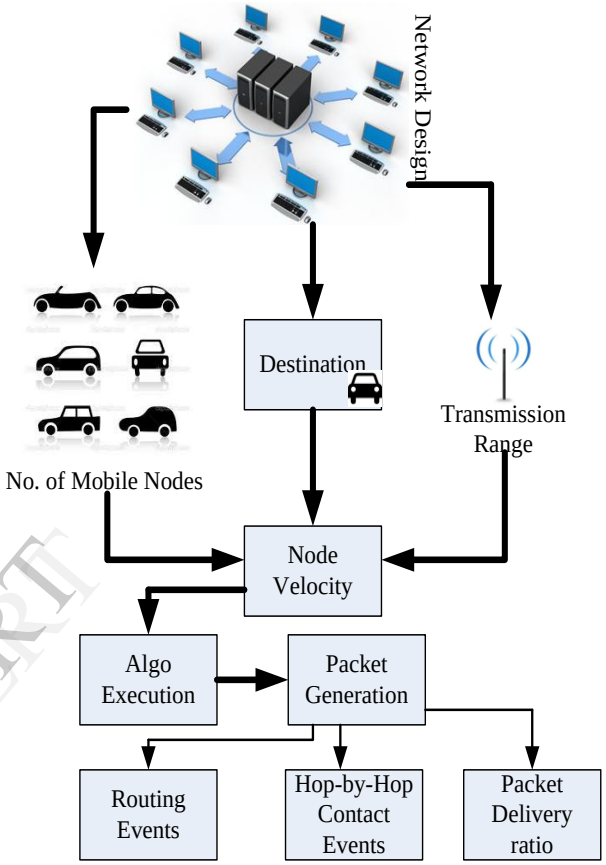


Figure 1 Schematic Illustration of proposed model

The current work, as shown in Fig.1, is addressed keeping dynamic topology in mind and all the possible security issues raised in the security protocol design of the mobile adhoc network. The proposed system provides a fair secure routing model in which malicious nodes in infected routes are stimulated to help forward bundles with secure protocols. In the proposed model, in order to achieve routing security, if and only if the bundles arrive at the destination node, the intermediate forwarding nodes can get acknowledged from the source node. Furthermore, for the failure of bundle forwarding, those intermediate forwarding nodes still can get good acknowledgement values from a trusted authority. Therefore, with this stimulation, the packet delivery performance of MANET can be improved. Moreover, in order to guarantee the feasibility of the fair secure routing model, the proposed system a verifiably encrypted signature technique to provide authentication and integrity protection. In order to prevent the overall performance degradation, i.e., low delivery ratio and high average delay, due to the malicious nodes in infected

routes in MANET, the hop-to-hop based secure routing and packet forwarding scheme is adopted. The basic strategy is to provide acknowledgement for intermediate forwarding nodes to faithfully forward packet. Generally, the intermediate nodes will get acknowledged for packet forwarding from the other nodes, and will take the same mechanism to acknowledge for their packet forwarding requests, by which the overall performance (i.e., high delivery ratio and low average delay) of the MANET can be assured. In the acknowledgement of node-to-node interaction phase if a packet is really relayed to the destination node, the source node will update the acknowledged routes to those intermediate nodes for forwarding. However, if the packet forwarding fails to reach the destination node, the source node won't acknowledge any nodes. Therefore, it is fair to the source node. For the intermediate nodes, although they can't get better update points for their forwarding in case they still can increase their good reputation values from the trusted authority. When the gaining factor is large, those intermediate nodes still feel fair for packet forwarding. In addition, since the provably secure short signature schemes are employed, the authentications from the signatures can provide strong witnesses. If an intermediate node didn't participate in forwarding, it can't get any acknowledged points. Therefore, from the above analysis, the proposed hop-to-hop secure routing scheme can provide fair security to the Mobile adhoc network. However, the updates are highly encrypted using public key from sender and private keys from destination node.

## V. ALGORITHM EXECUTION & RESULT

The proposed system is simulated on standard 32 bit Windows OS on Java Platform. Computer simulation is one of the most widely used way to evaluate the MANET routing protocols. Because it provides four main advantages – (i) it enables experimentation with large networks; (ii) it enables experiments with configurations that may not be possible with existing technology; (iii) it allows for rapid prototyping by significantly abstracting the complexity of the real system. Simulators enable the development and debugging of new protocols with reduced effort and (iv) it makes reproducible experiments in a controlled environment possible. The working of Secure Routing Protocol in MANET is explained is that messages in ad hoc network must be authenticated to guarantee the integrity and non-repudiation so that the protocol and nodes can be prevented against several kinds of attacks.

*Key Agreement Process between Neighbor Nodes:* A node joining a network requires sending key agreement messages to its neighbors to negotiate a shared secret key.

**Algorithm 1**: For node-to-node authentication of the Network Model

1. Begin
2. Input: Set of number of nodes
3. Output: Node destination
4. Sender node broadcasts a message indicating the negotiation request with neighbor nodes <Key_agreement_req, request_id, sender_address, $PK_S$ >
5. Sender node gets reply a message <Key_agreement_rep, request_id, sender_address, neighbor_address, $PK_N$ >
6. Generate a key Ks by using a secure random number generator,
7. Encrypt Ks with PKB (node B's public key) = encrypt PKB (Ks),
8. Send an offer message <KEY_PASS, encrypt PKB (Ks)> to B,
9. Wait ACK (acknowledgement) from B and check message integrity to finish the negotiation
10. Let node B receives the key passing message; it decrypts "encrypt $PK_B$ (Ks)" by its private key (pB) to get the shared key K. Then, node B sends the ACK message <KEY_ PASS_ ACK, request_id, $HASH_{Ks}$ (request_id)>
11. successful shared secret key negotiation,
12. END

Where $PK_S$ and $PK_N$ is the public key of the sender node and replying node, each node in a network has its own a pair of public key e and private key d following RSA Public-key Crypto-system by self-generation, and each node contains a list of neighbor nodes with records containing the information of a neighbor node including neighbor address, neighbor public key, and a shared secret key. This information is formed after the key agreement between two neighbor nodes to negotiate a pair of keys and a shared secret key.

*Route Request:* Route request (RREQ) is initiated by a source node (S) and then propagated by intermediate nodes until the message reaches its destination node (D).

**Algorithm 2**: Identification of the required bundle signature

1. Begin
2. Input: Set of number of bundle
3. Output: Identification of the required destination node and path to simulation the required bundle signature
4. Initialize the nodes, speed, radio range and bundle status
5. Get Encrypted bundle in array list
6. Set encrypted bundle in binary
7. Choose and get initial Personal credit account
8. Choose and set initial personal reputation account
9. Generate the create bundle
10. For {

Determine the no. of bundle values

Evaluate each signature of the nodes

}

11. Generate the receive bundle
12. For {

    Unique id of the nodes

    Add the authorized nodes

    Remove the unauthorized nodes

    }
13. Generate the forwarded bundle
14. Trusted authority has forwarded from sender node to receive nodes
15. if (Current Time < = Received time + Holding time) then

    {

        Forwarded Bundle to receive nodes

        }

    Else

        {

            If (encrypted bundle = null) then

            {Set the bundle status

            }}
16. Return bundle status
17. END

After identification of the required bundle signature, the system will also provide the security Certificate authority and node is forwarded to destination. Once the application is run must be select the no. of node, source, destination, speed, simulation and start the protocol. In the progress of the simulation, the framework will highlight the number of bundles has selected manually that much of bundle generation is displayed like as above figure and must be selected source and destination nodes. Figure 4 shows the simulation result where the public key is highlighted to be in encrypted form along with location of the mobile nodes too. The result also highlights the encrypted bundle.

| My Simulation[Java Applet] C:\program Files\java\jdk1.6.0\bin\javaw.exe | |
|---|---|
| The Public Key is | |
| Node N2 Co-ordinate (Location) | 20,382 |
| The Public Key is | |
| Node N3 Co-Ordinate (Location) | 354,90 |
| The Public Key is | |
| Node N4 Co-Ordinate (Location | 354,236 |
| The Public Key is | |
| Node N5 Co-Ordinate (Location) | 354,382 |
| The Public Key is | |
| Node N6 Co-Ordinate (Location) | 689,90 |
| The public Key is | |
| Node N7 Co-Ordinate (Location) | 689,236 |
| The Public Key is | |
| Node N8 Co-Ordinate (Location) | 689,382 |
| All Node are Initialized | |
| The Destination Node is | 5 |
| The Source Node is | 2 |
| Creating Bundle | |
| The Bundle Creates is | Bundle of N2 with Message Id 1 |
| Encrypting Bundle | |
| Get Signature of Bundle | |

Figure 2 Message authentications of Encrypted keys

Once run the application node message authentication of encrypted keys of certificate authority is providing for bundle signatures. After selecting the source and destination bundle nodes, the nodes must be forwarded one node to one node finally will reach the destination of the bundle signature. The above simulation shows highly secured communication with extremely less communication or network overhead, which is normally found in implementing complex cryptographic protocols.

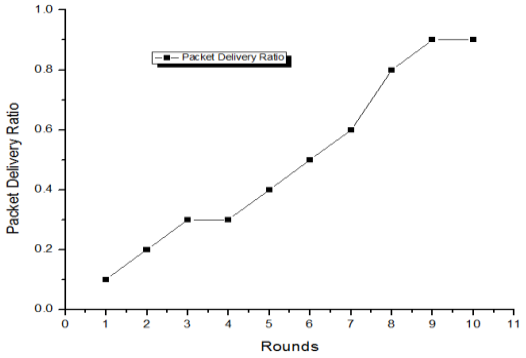


Figure 3 Packet Delivery Ratio

Different from the conventional protocol, the proposed protocol focuses on the fairness issue in Mobile adhoc

networks. Specifically, we propose a hybrid hop-by-hop interaction model with verifiably encrypted signature technique to stimulate the selfish mobile nodes to help forward packet. Fig.3 shows the result accomplished after performing the simulation study to see that the packet delivery ratio of the proposed system that is highly optimized while maintaining a better uniformity in the processing time. To achieve fairness, if and only if the packets arrive at the destination node, the intermediate forwarding nodes can get acknowledgement from the source node. Furthermore, for the failure of packet forwarding, those intermediate mobile nodes still can get good acknowledgement values from the trusted authority. Therefore, mobile nodes will be more confident in participating in packet forwarding.

## VI. CONCLUSION

As the available wireless networking and mobile computing hardware is now capable of fulfilling the promise of this technology. It is the need of the hour to design and develop routing protocols which should support the performance with endurance. The correct execution of these routing protocols is mandatory for smooth functioning of a MANET. A variety of protocols have been proposed targeted at securing MANETs but no performance comparison between these protocols has previously been available. In the presented work we have compared these protocols by highlighting their features, differences and characteristics. It can be summed up that each protocol has definite advantages and disadvantages, and can be appropriate for a particular application environment. From the discussion of the above results, we can safely conclude that the mobile ad hoc network is insecure by its nature: there is no such a clear line of defense because of the freedom for the nodes to join, leave and move inside the network; some of the nodes may be compromised by the adversary and thus perform some malicious behaviors that are hard to detect; lack of centralized machinery may cause some problems when there is a need to have such a centralized coordinator; restricted power supply can cause some selfish problems; and continuously changing scale of the network has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network. As a result, compared with the wired network, the mobile ad hoc network will need more robust security scheme to ensure the security of it. In the next section, we will survey several security solutions that can provide some helps to improve the security environment in the ad hoc network.

## REFERENCES

[1] Mishra, A., Nadkarni, K.M., "Security in Wireless Ad Hoc Networks," in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[2] Yadav, P., Gill, R.K., Kumar, N., "A Fuzzy Based Approach to Detect Black hole Attack," International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol-2, Issue-3, 2012

[3] Nand, P et al., "Performance study of Broadcast based Mobile Adhoc Routing Protocols AODV," DSR and DYMO. Wireless Pervasive Computing, 2007. 2nd International Symposium on Date of Conference, 2007.

[4] Johnson, D.B. et.al, "Dynamic Source Routing in Ad Hoc Wireless Networks", Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on Date of Conference, 2007.

[5] Lin, X. et al., "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks," Communications, 2007. ICC '07. IEEE International Conference on Date of Conference, 2007.

[6] Su, X. et al. "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks. Communications," ICC '07.IEEE International Conference on DateofConference, 2007.

[7] Jaafar, M.A. et al., "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment," Communications Magazine, IEEE Date of Publication, 2008.

[8] Singh, U. e.t.al, "Secure routing protocols in mobile adhoc Networks-A Survey and Taxonomy," Wireless Communications and Networking Conference, 2008. WCNC2008. IEEE Date of Conference, 2008.

[9] Francq, J. et al., "Error Detection for Borrow-Save Adders Dedicated to ECC Unit. Fault Diagnosis and Tolerance in Cryptography," 2008. FDTC '08. 5th Workshop on Date of Conference, 2008.

[10] Defrawy, K.E. et al. "Privacy-Preserving Location-Based On-Demand Routing in MANETs," Risks and Security of Internet and Systems, 2008. CRiSIS '08. Third International Conference on Date of Conference, 2008.

[11] Kurosawa, S. et al., "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" Networks, 2008. ICON 2008. 16th IEEE International Conference on Date of Conference, 2008.

[12] Thakare, A.N. et al., "Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks," Advanced Information Networking and Applications Workshops, 2009.WAINA'09.International Conference on Date of Conference, 2009.

[13] Sanzgiri, K. et al. "A Secure Routing Protocol for Ad Hoc Networks," Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th International Conference on Date of Conferenc, 2009.

[14] Crrepeau, C., et al., "A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes," Vehicular Technology, IEEE Transactions on Date of Publication: Jan.2009

[15] Qabajeh, L.K., et al. "A Scalable, Distributed and Secure Routing Protocol for MANETs", Computer Technology and Development, 2009. ICCTD '09. International Conference on Date of Conference, 2009.

[16] He, F. et al, "S-MAODV: A Trust Key Computing Based Secure Multicast Ad-hoc On Demand Vector Routing Protocol,"Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on Date of Conference, 2010.

[17] Mondal, A.K., "The Success of Data Transmission in Multipath Routing for MANET", Informatics in Control, Automation and Robotics (CAR), 2010 2nd International Asia Conference on Date of Conference, 2010.

Najiya Sultana has 5 years teaching experience at degree level. She has completed MCA in 2005 and M. Phil. In 2010. She is pursuing Ph. D. from Rajasthan Vidyapeeth University, Udaipur. She has attended 5 international conferences and 2 national conferences. She is a member of CSI. Her research areas of interest are Ad Hoc networks, network security and security protocols.

Prof. Shiv Singh Sarangdevot is working as a Vice Chancellor of Janardan Rai Nagar Rajasthan Vidyapeeth University, Udaipur. He has completed Doctor of Philosophy in Computer Science, Master of Computer Application, and Human Resource Management. He has 26 years of teaching experience. He has also 10 years of wide industrial experience with rich 21 years in research domain. His area of specialization includes Internet & E-Commerce, Software Engineering, ERP and SAP, Research Techniques, Artificial Intelligence, and Networking. He has also published 8 books and 78 research papers till date.