ISSN (online) : 2277-5390
ISSN (Print) : 2277-5382

Reputation based routing protocol with improved performance

Anjali[1], Parminder Kaur[2]

ECE Department, SSIET, Derabassi, Punjab, INDIA
anjali51280@gmail.com parmindersandal@yahoo.com

Abstract

Objectives: Due to the advancements in the technology, security while transmission becomes a crucial part. So there is a need to design a new protocol that is more efficient than the traditional protocol, and should consider both security and packet delivery ratio along with some other parameters. With this intention, a new technique is proposed which considered the data rates and the security issues.
Methods/Statistical analysis: An improved version of HRARAN protocol is used in order to obtain a secure and reputed transmission in a network which is based on public key cryptography and reputation techniques. Reputation value of a node is used to know whether the node is able to cooperate in a network or not which is calculated by the past behavior of individual nodes. Thus, in such case a cooperative node in the network has highest reputation value. Value in the routing table upgrades after packet reaches at the destination.
Findings: Traditional approach does not perform accordingly in terms of accuracy and packet delivery ratio, which is only 62.3 as compared to the proposed approach in which PDR is high i.e. 76.3. Moreover, PDR defines the number of packet reach at the destination and it can be concluded that in the proposed approach packets reach more in improved HRARAN. Considering another parameter i.e. packet loss in the existing and proposed HRARAN is 754 and 474 respectively which concludes that accuracy of the improved HRARAN is high.
Improvements/Applications: The protocols can be improved by:

- Increasing number of quality parameters in order to selecting the best path.
- Optimization algorithms can be employed for finding out the optimized path for routing.

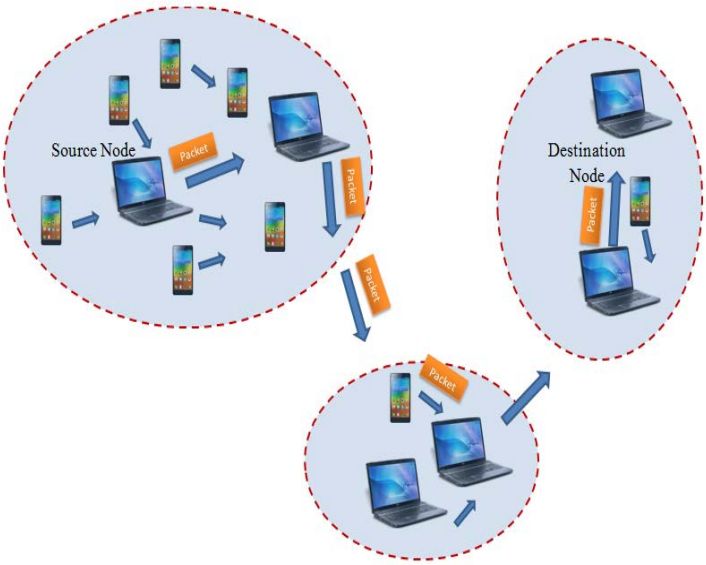
Keywords: *Reputation value, packet loss, MANET, HRARAN, routing protocols, path loss.*

Introduction

Traditional network follows fixed infrastructure to send data packets from source to destination. But with the advancements in the wireless networks, devices are communicate with each other without using fixed infrastructure or dedicated topology. Owing to this, MANET has been used ad hoc network for the communication. With the term ad hoc means uncertain structure where communication is not centralized [1]. All in all MANET worlds fixes the problem of having fixed infrastructure so that communication can be possible in variable environment. MANET is a network which is self-organized consisting mobile routers and associated hosts [2]. These hosts are connected through the wireless links. The main idea behind proposing MANET is to allow routers i.e. mobile devices, nodes to move freely randomly and they organize themselves subjectively. Due to this network of wireless topology has been changed rapidly. In such network, data hops from one device to another device till it reaches at the destination point. So that network has to be updated instantly and automatically on on-demand basis to keep nodes connected. At the time of linking or removal of a node in the network, topology changes accordingly. Each node in the network has taken the responsibility of packet forwarding, routing along with other network operations by themselves [3]. In wireless network, individual node treated as a router and changes its topology where the availability is not always taken as guaranteed. Furthermore path between two nodes are also not taken as for guaranteed in case of malicious attack. In MANET devices such as laptops, PCs, Cellular phones are connected with ad hoc communication capability link to form a network shown in the Figure 1.

ISSN (online) : 2277-5390
ISSN (Print) : 2277-5382

Figure 1. Routing in MANET



Link attacks can happen in case of wireless links. Some of the link attacks are passive eavesdropping; active interfering etc. Thus there is a requirement of proposing a security solution which must provide services like:

- Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Availability

On the whole, security is a major concern in case of communication between ad hoc networks. In the ad hoc networks two things that need to be considered are protection of routing functionality and protection of data in transmission i.e. secure packet forwarding [4]. In order to protect wireless network two types of protection techniques can be considered such as proactive and reactive. In proactive technique, prevention from attacker can be handled through applying cryptographic techniques before transmission. Alternatively, Reactive works after transmission of packet at the receiver side by detecting threat and then react accordingly [5].

Security attacks against routing in MANETs

Basically, attacks can be identified in terms of two categories named as passive attacks and active attacks in MANET. In case of passive attacks, attacker can listen and retrieve the vital information of the data packets. Example can be considered in such case is traffic monitoring attack. Thus the main idea is to get information about the parties involved in the communication and functionality. As a result it monitors the communication but do not alter the network [6]. Basic functionality of the network remains as it is. On the other hand, active attack has been performed in order to interrupt the functionality of routing in MANET. Active attack is performed by the malicious node [7].

- **Modification attacks**- This type of attack is special Denial-of-Service attack which happens to interrupt the entire routing function. In such attack source routes are altered in the header of the routing packet. Such type of attack is only effective if intermediate nodes have been included in the packet header [8]. For example- DSR.
- **Impersonation attacks-** In this type of attack, attacker or malicious node behaves like the receiver node and uses the IP address of the receiver in outgoing routing packets. Spoofing is another term used for this attack. Thus malicious node receives all the packets which were meant for the other node [9].
- **Fabrication attacks**- Malicious attacker attempts to set forged routes and make routing table of neighbor node jam-packed. Owing to this, new registration of the routes cannot enter. This type of attack is also known as DoS attack. It mostly attacks on table driven routing protocols where table needs to be updates in the network [10].

ISSN (online) : 2277-5390
ISSN (Print) : 2277-5382

- **Wormhole attacks** - It is a most rigorous attack that happens on the MANET routing. In this type of attack, one malicious node grabs packet and tunnel it to the next malicious node which is located several hops away. Thus from that node, it forwards the node to the neighboring nodes. Owing to this it behaves as if two endpoints are neighbors but in actual they are far away from each other. Consequently, this strategic placement of a wormhole will be treated as helpful route in the network. Due to which most of the traffic will follow this route. So once the wormhole link has been established by the malicious node in the network, further attacks can be possible in order to disturb communication [11-12]. Moreover, confidential communication can be lost.
- **Selfish behavior-** This type of attack is not considered as bad intention attack or it does not harm the communication in the network. This type of node does not cooperate in the communication and make offline itself by switch to the sleep mode [13]. Generally it switches its mode when it does not taking part in the network communication. This node does not affect the network but lead disturbance. For example, if in the communication there is only two nodes in the communication link between two MANET, in such case no communication will be taken place.

Routing protocols

There are numerous routing protocols available for ad hoc network which are based on the mechanism of updating routing table and according to the topology of the network [14-17].

According to mechanism of updating

- **Proactive**- Proactive protocol is also considered as table driven protocol in which it requires information of the nodes all time to maintain valid routing tables.
- **Reactive-** It is also known as on-demand routing where the table is not maintained regularly of all destinations. At the time of sending packet to the destination it checks the table with an active route to the destination. If so it sends packet but if not then the selected node must generate a route to the required destination.
- **Hybrid-** It is a combination of proactive and reactive routing. In between nodes within individual clusters it uses reactive (proactive) and between clusters it uses proactive (reactive).
- **Geographic-** In this method location of the node is considered as their address and then precede data packet to the destination. It is most efficient technique in any-to –any communication as it maintains neighbors of individual nodes.

According to topology of network [18-19]

- **Flat based routing-** In such type of routing each node in the network plays equal role. Due to which they can establish a route by local operation and can provide information feedback to the nodes easily. But in the large network it might be difficult for obtaining valid path which leads to high delay and network spending. Consequently this problem can be solved by hierarchical based routing mentioned next.
- **Hierarchical based routing-** In such type of routing protocol all the available nodes are divided into clusters referred as clusters. Thus each cluster picks a cluster head which will obtain the packet from the nodes and forwards to the destination. As a result, this will break down the number of nodes participating in routing. All in all network stability will be increased.

Background

The security of nodes while selecting a route for data selection is one of the main issues in wireless networks [20]. Security plays an important role for the system to be reliable and efficient. In the earlier techniques that ensure security of the route selected for the transmission of data the emphasis was laid on the reputation of the nodes. In these conventional techniques first the reputation of the nodes was checked and the selection of the route is done. After the selection of the route the reputation of the each node is updated after each route selection that made the system cumbersome. A new technique is to be introduced that can efficiently select the route so that high security to the nodes is provided and the data can be reliably transmitted from the source node to the destination node.

ISSN (online) : 2277-5390
ISSN (Print) : 2277-5382

Proposed work

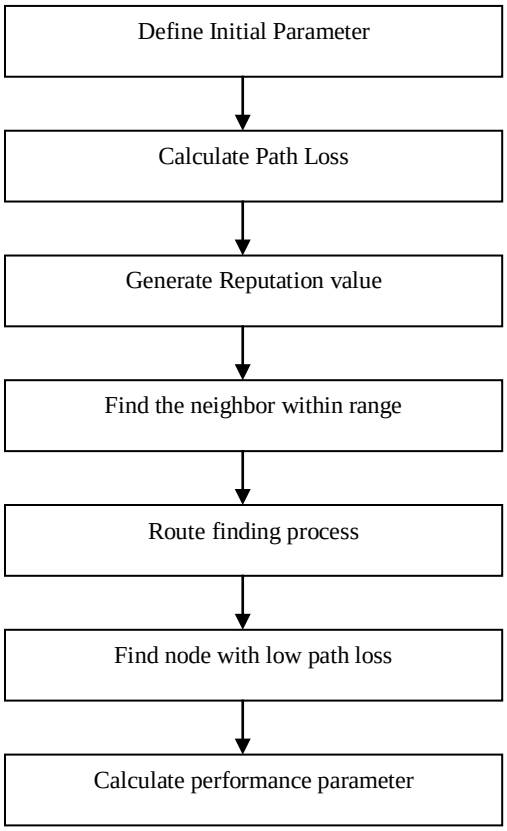
In the proposed technique the security of the system is enhanced by changing the criterion for route selection. In the earlier techniques only the reputation of nodes was considered for route selection but in this proposed technique certain quality of service parameters are also considered along with the reputation of nodes.
The main factor that will be done in the proposed section will be basically reputation as it was in the previous work and the factors which will come along with it will be path loss model of the wireless communication and the RDC means radius dependent communication.

- Reputation
- Path loss
- Radius dependent communication (Range)

Methodology

As in the traditional approaches, reputation value is the only factor that has been considered but in the proposed technique along with reputation value, path loss and RDC parameter is also considered. Methodology for the proposed technique is shown in Figure 2.

Figure 2. Block diagram of Improved HRARAN



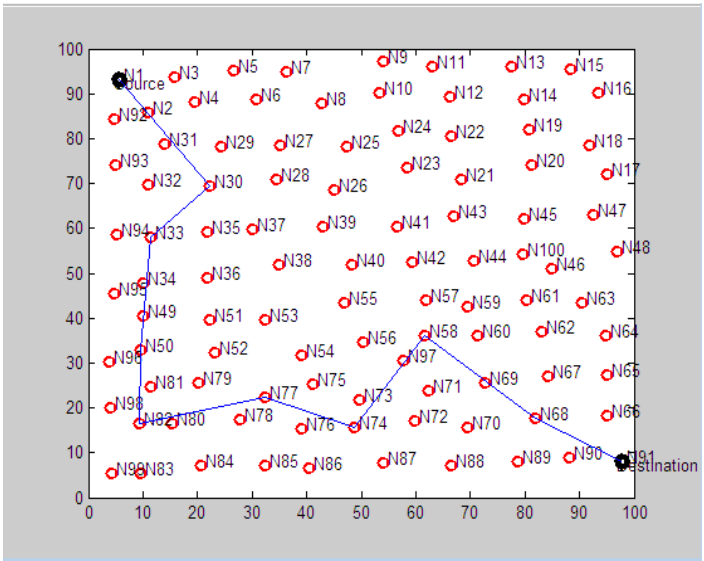
1. Initially parameters have been selected for the evaluation of the nodes in the network.
2. After initialization, path loss is calculated to check the accuracy or reliability of the route.
3. After evaluation of path loss, generate reputation value of each node in the network. Reputation value provides help in selecting consistent route for the transmission of packets from source to destination.
4. Find neighbor which is available in the range after generation of reputed value of individual nodes.
5. Locate route from source to destination in the network.
6. Now find a node having less number of path losses So that more number of packets can reach at the destination.
7. Lastly determine performance parameter like PDR, packet loss, distance and threshold value.

ISSN (online) : 2277-5390
ISSN (Print) : 2277-5382

Results and discussion

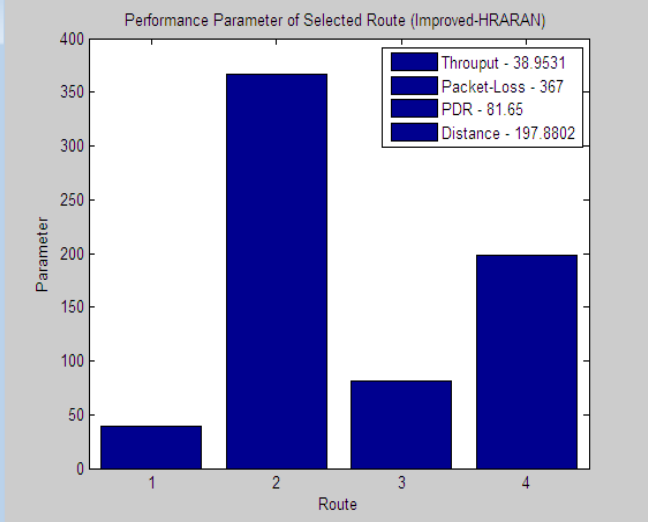
In this section, results have been evaluated using number of nodes in the network. Performance parameters like throughput, packet delivery ratio, packet loss, distance have been calculated to show that proposed technique outperforms in comparison with traditional approach. For the evaluation part; number of nodes are 100 in the network from which node 1 is treated as source and node 91 is the destination. Thus from node 1 to 91 a route has been calculated for the transmission of packets shown in Figure 3.

Figure 3. Selection of trusted path from source to destination.



Different performance parameter is evaluated using proposed technique. These parameters are used to show the quantitative value of improved HRARAN (Figure 4).

Figure 4. Evaluation of performance parameter of improved or proposed approach.



ISSN (online) : 2277-5390
ISSN (Print) : 2277-5382

Figure 5. Comparison between traditional and proposed approach

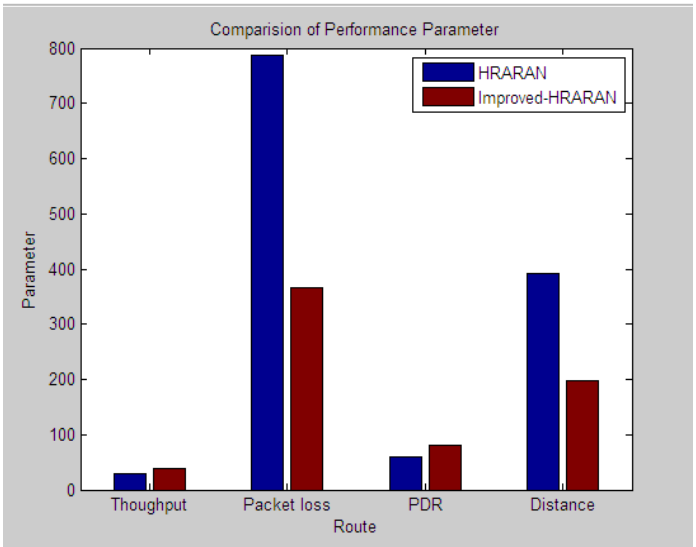


Figure 5 represents the comparison based on different performance parameter to estimate which technique is better and efficient. Moreover to identify which technique is able to send multiple packets at the destination in less distance and high throughput.

Conclusion and future scope

At the time of routing, selection of route depends on the path reputation which is based on the reputation and trust values of each node in the network. For the future directions, HRARAN can be enhanced in terms of quality of service and accuracy. Maximum availability of the node in the network can also be improved.

References

1. C. Atheeq, M.M.A Rabbani. Secure data transmission in integrated internet MANETs based on effective trusted knowledge algorithm. *Indian Journal of Science and Technology*. 2016; 9(47), 1-7.
2. A. Vangili, K. Thangadurai. Detection of black hole attack in mobile ad-hoc networks using ant colony optimization – simulation analysis. *Indian Journal of Science and Technology*. 2015; 8(13), 1-10.
3. C. Joseph, P.C. Kishoreraja, R. Baskar, M. Reji. Performance evaluation of MANETs under black hole attack for different network scenarios. *Indian Journal of Science and Technology*. 2015; 8(29), 1-10.
4. A. Shitalkumar, V.T. Raisinghani. LUNAR: Working and performance evaluation in MANETs. *Indian Journal of Science and Technology*. 2016; 9(45), 1-18.
5. J. Deny, M. Sundhararajan. Multi modal biometric security for mobile ad-hoc networks and its applications. *Indian Journal of Science and Technology*. 2016; 9(42), 1-6.
6. K. Vijayakumar, K. Somasundaram. Study on Reliable and Secure Routing Protocols on Manet. *Indian Journal of Science and Technology*. 2016; 9(14), 1-10.
7. A. Hinds, M. Ngulube, S. Zhu, H. Al-Aqrabi. A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET). *International Journal of Information and Education Technology*. 2013; 3(1), 1-5.
8. P.T. Kasthuri, M. Sundararajan. Performance efficiency of OLSR and AODV protocols in Manets. *International Journal of Information and Education Technology*. 2015; 8(14), 1-4.
9. V. Kärpijoki. Security in Ad Hoc Networks. *Seminar on Network Security*. 2000, 1-16.
10. G. Usha, S. Kannimuthu, G. D. Karthik. Survey of single and cross layer security in MANET. *International Journal of Information and Education Technology*. 2016; 9(41), 1-9.
11. S.S. Jabamani, E. Rajinikanth. Integrity key based mechanism to debase packet dropping in MANETs. *International Journal of Information and Education Technology*. 2016; 9(14), 1-4.
12. I. Vijaya, A.K. Rath, B. Puthal. Exploration of security threat analysis in Wireless Mobile Adhoc Network. *International Journal of Information and Education Technology*. 2016; 9(35), 1-11.

ISSN (online) : 2277-5390
ISSN (Print) : 2277-5382

13. D. Bandral, R. Aggarwal. Simulation analysis of AODV and DSDV routing protocols for improving quality of service in MANET. *International Journal of Information and Education Technology*. 2016; 9(32), 1-5.
14. A. Nedumaran, V. Jeyalakshmi. CAERP: A congestion and energy aware routing protocol for Mobile Ad Hoc Network. *International Journal of Information and Education Technology*. 2015; 8(35), 1-6.
15. T. Ahamad , A. Aljumah. Detection and defense mechanism against DDoS in MANET. *International Journal of Information and Education Technology*. 2015; 8(33), 1-4.
16. D.S. Kumari, K.T. Sikamani. Communication based clustering to detect selfish nodes in MANET. *International Journal of Information and Education Technology*. 2015; 8(20), 1-6.
17. S.J. Sultanuddin, A. Hussain. Shortest and efficient multipath routing in Mobile ad hoc Network (MANET). *International Journal of Information and Education Technology*. 2016; 9(45), 1-9.
18. M. Vinoth, S. Omkumar. LOMAN – A new design for implementation of the MANET protocol over IOT environment. *International Journal of Information and Education Technology*. 2016; 9(35), 1-7.
19. G. Suseendran, A. Sasikumar. Secure intrusion-detection system in Mobile Adhoc Networks. *International Journal of Information and Education Technology*. 2016; 9(19), 1-6.
20. M. Angu, S. Anand. Detection and avoidance of gray hole attack in Mobile Ad-Hoc Network. *International Journal of Information and Education Technology*. 2016; 9(47), 1-6.

The Publication fee is defrayed by Indian Society for Education and Environment (iSee). www.iseeadyar.org

Citation:

Anjali, Parminder Kaur. Reputation based routing protocol with improved performance. *Indian Journal of Innovations and Developments.* 2016; 5(12), December.