SECURE DATA TRANSMISSION THROUGH NODE-DISJOINT ON DEMAND MULTIPATH ROUTING IN MANETS

Y. Vasudeva Reddy
Research Scholar, Department of Computer Science, Rayalaseema University, Kurnool, India

M. Nagendra
Department of Computer Science and Technology, Sri Krishnadevaraya University, Ananthapuramu, India

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are the wireless networks which can be deployed instantly without requiring any fixed wired infrastructure. MANETs are specifically very much useful in military, commercial and civilian applications. Since infrastructure less MANETs have dynamic topology and battery powered mobile nodes, it is a challenging task to provide secure data transmission between any pair of nodes in MANET. Multipath on Demand Routing is one possible solution to provide security in MANET. This paper proposes a new method (SDNMR) of providing secure communication by integrating trust based mechanism with multipath on demand routing approaches in MANETs. The simulation analysis of proposed method reveals the facts that the method provides significant security to the data compared to previous related work.

Keywords: Data Security, Mobile Ad Hoc Networks, Multipath Routing, Node-disjoint, Protocol Design.

Cite this Article: Y. Vasudeva Reddy and M. Nagendra, Secure Data Transmission through Node-Disjoint on Demand Multipath Routing in MANETs, International Journal of Computer Engineering and Technology, 10(2), 2019, pp. 135-147.

http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=10&IType=2

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are popular due to their rapid deployment as and when there is a need of infrastructure less temporary complete wireless network [1]–[3]. As shown in Fig.1, MANET is a multi-hop wireless network in which the nodes act as both hosts and routers i.e., nodes forward the packets of other nodes which present between source and destination hosts. Routing is an important networking function which finds the routes between source and destination nodes before data transmission takes place between them. The nodes in
MANETs are moving constantly from one location to another and it results in dynamic topology of MANET. Moreover, the nodes are constrained by their battery power. Hence, facilitating routing in MANETs is a challenging task.

All the routing protocols of MANET can be classified into three categories: proactive (static), reactive (on-demand) and hybrid protocols [4]. Proactive routing protocols like DSDV [5], WRP [6], CGSR [7], GSR [8], etc. establish routing paths between each pair of nodes in MANET before data transmission takes place. To maintain the routes according to the changes in network topology, the nodes periodically exchange topology information which is an overhead in proactive routing approach. Reactive routing protocols as ABR [9], TORA [10], DSR [11], AODV [12], etc., discover the route only when there is data transmission between a pair of nodes. Moreover, the routes are maintained as long as data transmission takes place. Once the data transmission is completed, the route is no more maintained. Reactive routing protocols discover the routes using query-reply based approach. Hybrid routing protocols like ZRP [13] are developed using merits of both static and dynamic routing protocols. Irrespective of type of routing protocol used in MANET, there exist some common and/or specific routing attacks [14]–[20]. Also, several solutions to solve security problems in MANETs have been proposed. One possible solution is to use multipath routing instead of traditional unipath routing in MANET.

Another classification of MANET routing protocols is based on number of paths used for data transmission: unipath and multipath routing protocols. Only one route is used for sending data from source node to destination node in case of unipath routing. On the other hand, atleast two different routing paths are used for data transmission between source and destination nodes if multipath routing scheme is used. Multipath routing schemes provide more security than unipath routing schemes because an attacker has to compromise at least one node in each path to collapse the security system of MANET. Multipath routing protocols are two types: node-disjoint and link-disjoint protocols. No two paths must have a common node in node-disjoint routing. Similarly, no common link is present between two or more paths in link-disjoint multipath routing protocols. Some of the node-disjoint protocols are [21]–[23] and a few link-disjoint protocols are [24], [25]. For security purposes, node-disjoint multipath routing protocols are preferable than link-disjoint multipath routing protocols because if the attacker destroys the common link then multiple paths will be affected in link-disjoint multipath routing protocols. Node-disjoint multipath routing protocols are also considered as link-disjoint multipath routing protocols but not vice versa. The proposed secure method, SDNMR (Secure Data Transmission through Node-disjoint Multipath Routing protocol), is based on node-disjoint on-demand multipath routing scheme.

Figure 1 Mobile Ad Hoc Network

http://www.iaeme.com/IJCET/index.asp
Secure Data Transmission through Node-Disjoint on Demand Multipath Routing in MANETs

Many different protocols of security through multipath routing [26]–[34] exist in the literature. It is observed from the in-depth analysis of literature that most of the protocols were proposed to follow trust based security measurements to maintain multiple paths. A little work as [42] is providing both route security and data security. But unable to address attacks by selfish nodes which drop the data packets to save their battery power. With this motivation, this proposes a protocol SDNMR that provides security in the discovery of all distinct node-disjoint multiple paths from source to destination and also during the data transmission between them. Unlike previous work, SDNMR predicts the remaining battery power levels of nodes in addition to packet drop ratio and accordingly it chooses the routes to send the data. The general framework of the proposed secure work provides flexibility in extending the work with any trust model.

This paper content is organized as follows: motivating literature work is discussed in section 2 and the mathematical model of proposed work SDNMR is presented in section 3. SDNMR evaluation is analysed in section 4 and the paper ends with conclusion in section 5.

2. RELATED WORK

Since one of the important applications of Mobile Ad hoc Networks is military communications, secure transmission of data obtained significant attention by the research community. Most of the researchers suggested to use multipath routing schemes to achieve load balancing and security in MANET. Specifically, node-disjoint on-demand multipath routing protocols are recommended by researchers [17]–[20], [35]–[37].

There exist various types of security attacks in MANETs and our previous work [38] presents a detailed survey analysis on it. It is hard to detect internal malicious nodes participating in DoS attacks. However, multipath routing schemes are most securable than unipath routing protocols in controlling DoS attacks and minimizing the data loss.

The SRP protocol proposed in [39] uses symmetric cryptographic method to secure route discovery process of on-demand routing protocols but unable to discover all existing node-disjoint multiple paths that exist between source and destination nodes in MANET. The protocol in [40] discovers all distinct node-disjoint multiple paths with certain hop count between nodes but route request messages cause delay in processing. SecMR protocol in [41] solves the limitations of [39] and [40] such that it discovers all distinct node-disjoint multiple paths with certain maximum hop count and no additional delay than normal operation of on-demand routing protocol. SecMR protocol protects the route discovery process from malicious nodes but data security is not addressed. All these work [39–41] protect the MANET from DoS attacks by malicious nodes by securing the multipath routes discovery process. Some nodes in MANET intentionally drop the data packets for saving their battery power or other reasons. These kinds of selfish nodes are difficult to be detected by the security system. The work [39–41] cannot address this attack. Our work is inspired from [41] but we address the problem of data security from selfish nodes after route discovery process.

For data security purpose, our protocol integrates a trust based security scheme with the asymmetric cryptography scheme used in multipath route discovery process. There exist different schemes of trust based security models [29], [30], [33], [34] in the literature which differ in node trust metrics used in process and all these work discover securable node-disjoint multiple paths and also not addressing data security during transmission. But our protocol uses trust based metrics for data security purpose and not to discover the paths. Clearly, the proposed work in this paper uses asymmetric cryptographic principles to protect route discovery process and route maintenance. During data transmission after the route discovery process, the proposed protocol, SDNMR, uses trust based metrics to control data loss due to selfish node attacks. Most recent work which is more relevant to our work is presented in [42].
but that work used trust based route discovery process followed by cryptographic based data security. Moreover, it is mentioned that the trust value of each node is calculated as a discrete value of either 0 or 1. All the previous work mentioned in the paper, did not address the attacks by selfish nodes which drop the data packets to save their battery power. With this motivation, our proposed protocol SDNMR, calculates trust value for each node based on number of packets received and forwarded. Unlike previous work, SDNMR predicts the nodes remaining battery power levels and accordingly decide the amount of data to transmit through the paths. SDNMR assumes that the nodes with low battery level have high probability to drop the data packets and so SDNMR decreases the number of data packets through the path that have low battery power. The detailed framework of proposed protocol is presented in section 3 and simulation analysis indicates that the proposed work shows significant improvement over the previous related work mentioned in the paper.

3. DESIGN OF PROPOSED PROTOCOL, SDNMR

This paper presents a novel security protocol called SDNMR which is applicable with on-demand routing approach. Basic versions of DSR and AODV discover multiple paths between source and destination nodes but they use only one path for data transfer. To experience the full benefits of multipath routing like load balancing and security, the routing protocol must use all existing distinct node-disjoint paths for data transfer. With this observation, our protocol SDNMR is designed to discover and use all possible distinct node-disjoint multiple paths between source and destination. Moreover, SDNMR discovers most secure and authenticated routes using asymmetric cryptographic scheme and the data transmission is secured with trust based scheme. Specifically, SDNMR calculates trust value of each node by considering packet drop ratio and remaining battery power.

3.1. Assumptions

While designing the proposed protocol SDNMR, it is assumed that there are ‘n’ number of nodes present in the MANET. Each node in MANET is capable of acting as both router and host. As there is no specific centralized node to monitor networking functionalities like routing, security, etc. each node takes care of itself. Often it is possible that source and destination hosts are separated by numerous intermediate nodes, and during data transfer between them, each node has to trust other nodes. The MANET uses on-demand routing scheme which finds routes between source and destination hosts only when there is data transfer between them and the routes are alive until all the data transmission is completed. On-demand routes are discovered using query-reply approach and it is assumed that only destination node gives route reply message and all other intermediate nodes do not reply but simply forward the route request. This is assumed so that all possible existing distinct node-disjoint multiple paths can be discovered between source and destination nodes. Specifically, the MANET uses node-disjoint multipath routing scheme for security reasons.

3.2. SDNMR Description

The proposed SDNMR protocol discovers all possible distinct node-disjoint on-demand multipath routes constrained to certain maximum hop count, through which the data can be transmitted from source to destination node. During routes discovery process, necessary security measurements are taken to avoid DoS attacks by malicious nodes. Also, all the intermediate nodes present between source and destination nodes are authenticated such that the security problems like man-in-the-middle attacks [43] can be prevented. Hence, SDNMR uses a simple light weight trust based secure mechanism to control the loss of data packets by such selfish nodes. During routes discovery process, SDNMR also calculates each route trust
value as the sum of trust values of all the nodes in that route. SDNMR transmits the data according to the trust values of routes i.e. a route with higher trust value carries more number of data packets than a route with lower trust value. During data transmission, SDNMR periodically calculates each route trust value and accordingly data packets to be transmitted through those routes are determined. Any kind of trust based model can be included with the proposed secure route discovery process. This kind of general framework of SDNMR provides flexibility to experiment with different trust models.

As the first step, in SDNMR, all the nodes have to authenticate their one-hop neighbourhood nodes using asymmetric cryptography scheme. If \( n_i \) is a node ‘i’ then it can have a pair of public and private(secret) keys as \( [PK_i, SK_i] \) respectively using asymmetric cryptography system [44]. All the nodes share their public key \( PK_i \) with other nodes through public key certificate \( CERT_i \) issued by certificate authority. The key generation schemes and certificate authority schemes are beyond the scope of the paper and there are several such schemes as [45]–[47]. The certificate \( CERT_i \) of node \( n_i \) also contains its unique identifier \( ID_i \) issued by certificate authority. The size of \( ID_i \) depends decides the maximum number of nodes that can present in MANET. For example, using a 2-byte \( ID_i \), a maximum of 65,535 nodes can be addressed.

Each node \( n_i \) has to share its information in the form of \( CERT_i \) with its one-hop neighbours by broadcasting a signed message \( Msg_i \) periodically. The structure of message \( Msg_i \) at time ‘t’ is \( <t, ID_i, sig_i(t, ID_i), CERT_i> \) where \( sig_i(t, ID_i) \) is the digital signature of node \( n_i \) having identifier \( ID_i \) and signed at time ‘t’. All the nodes can verify their one-hop neighbours by verifying signatures of each other. The time period for neighbourhood verification depends on system parameters such number of nodes, connectivity, topology changes, etc. Once the neighbourhood verification stage is over, each node \( n_i \) will have its one-hop neighbour list \( N_i \) at time t.

Once each node \( n_i \) has its one-hop authenticated neighbour list \( N_i \), the route discovery process will be initiated by a source node S to the destination node D. Since our protocol SDNMR is designed to work with on-demand routing protocols, when a source node S has some data to transfer to a destination node D, then node S first checks for route to D in its routing table. If no route is found to D, then node S composes a route-request message \( RREQ_{S,D} \) as follows:

\[
RREQ_{S,D} = <ID_S, ID_D, SEQ, HopCount_{current}, HopCount_{max}, E_{PK_D}(Key_{S,D}), List_{Trust}, List_{Exclude}, List_{Route}, List_{NextHop}, hash_{K_{Sys}}(ID_S, ID_D, SEQ, HopCount_{max})>
\]

Here \( ID_S \) and \( ID_D \) are the identifiers of source node S and destination node D. SEQ is the unique sequence number generated for each new route request message so that duplicate messages can be discarded. Current hop count and maximum hop count are tracked using \( HopCount_{current} \) and \( HopCount_{max} \) respectively. The value of \( HopCount_{max} \) is fixed by source node S based on current knowledge on network connectivity, node density, etc. and it is not modified by any other intermediate node present between S and D. But \( HopCount_{current} \) value is incremented by 1 each time an intermediate node forwards \( RREQ_{S,D} \). Initial value of
HopCountcurrent is 0 which is set by source node S. When HopCountcurrent value reaches HopCountmax, the route request message RREQS,D cannot be forwarded by intermediate nodes. KeyS,D is the sessional key shared by both source and destination nodes S and D respectively. The source node S randomly selects and encrypts the session key KeyS,D using public key PKD of destination node D such that D is the only node which can decrypt the KeyS,D and the intermediate nodes cannot decrypt the KeyS,D as it can be decrypted by only private key of node D which is not available with the intermediate nodes. EPKD(KeyS,D) is the encrypted session key used by both nodes S and D for secure data transmission. ListRoute is dynamically updated list by intermediate nodes that become the part route from S to D. Similarly, ListExclude is the dynamically generated list by the intermediate nodes present between S and D and this list specifies the nodes that are excluded from being part of route discovery of a particular thread of route request query. The two lists ListRoute and ListExclude are containing only IDS and they are incrementally populated by intermediate nodes during route discovery process. TrustRoute is the aggregated trust value of a route which is initiated by source node S. First, node S adds its trust value to TrustRoute and then TrustRoute is updated by each intermediate node that becomes the part of route. ListNextHop is the list of nodes which is dynamically populated by intermediate nodes that become next hops of query. Static data like (IDS,IDD,SEQ,HopCountmax) is hashed with session key KeyS,D such that the data is not maliciously modified by intermediate nodes.

hashKeyS,D(IDS,IDD,SEQ,HopCountmax) is the hashed key function of static data (IDS,IDD,SEQ,HopCountmax).

Each node ni has a trust value at time ‘t’ Trusti,t which is calculated as follows:

\[ Trust_{i,t} = w_1 \frac{PackFwd_{i,t}}{PackRe_{i,t}} + w_2 RP_{i,t} \]

where PackRe_{i,t} is number of packets (both data and control packets) received by node ni upto time ‘t’ and PackFwd_{i,t} is the number of packets forwarded by node ni upto time ‘t’. The parameter RP_{i,t} indicates the remaining power of node ni at time ‘t’. Two weight parameters w1 and w2 are used in trust calculation and the values are set according to network conditions and application requirements. If more secure path is required the weight of w1 can be increased or if long lasting route is required then the weight of w2 can be increased. In our simulations, we gave equal weight to both parameters.

The value of RP_{i,t} is calculated as follows:

\[ RP_{i,t} = IE_{i,t} - EC_{i,t} \]

where IE_{i,t} is the initial energy of node ni and EC_{i,t} is the energy consumed by ni upto time ‘t’ since the node is turned on. The value of EC_{i,t} is EC_{i,t} = EC_{i,t} + EC_{x,t} where EC_{x,t} is the energy consumed on receiving packets upto time ‘t’ and EC_{x,t} is the energy used to transmit the packets upto time ‘t’.

When an intermediate node receives a RREQS,D packet the node first hashes the packet and stores the hashed value in its routing table for some time. Meanwhile, if the same RREQS,D
Secure Data Transmission through Node-Disjoint on Demand Multipath Routing in MANETs

packet is received, it will find the same hash value in its routing table and drops the packet. But if a different instance of \(RREQ_{S,D}\) packet is received by the node then definitely its hashed value will be different because \(List_{Route}\), \(List_{Exclude}\) and \(List_{NextHop}\) values are different. This way an intermediate node is not prevented from calculating different paths towards destination node D. All existing possible distinct node-disjoint multiple paths will be discovered. Since the proposed protocol SDNMR has to find node-disjoint paths, each intermediate node checks whether any common node is participating in two or more paths by checking \(List_{Route}\) and \(List_{Exclude}\). Also, when an intermediate node \(n_i\) receives a \(RREQ_{S,D}\), it checks whether its identifier \(ID_i\) is present in received \(List_{NextHop}\) and checks whether the node identifier from which \(RREQ_{S,D}\) is received is the last one in the list \(List_{Route}\) and belongs to its authenticated neighbours list \(N_i\). If any one of these checks fail, the node \(n_i\) drops \(RREQ_{S,D}\). If the node \(n_i\) processes \(RREQ_{S,D}\) then it simply increases \(HopCount_{current}\) by 1 and checks the new value crosses \(HopCount_{max}\). If so, the packet will be dropped, otherwise it will append its identifier \(ID\) to the \(List_{Route}\) and forwards to its neighbours. The node \(n_i\) also updates the \(List_{Exclude}\) by appending all the node identifiers present in the received \(List_{NextHop}\) into \(List_{Exclude}\) to eliminate duplicate processing of packet \(RREQ_{S,D}\).

When the destination node D receives the \(RREQ_{S,D}\), it decrypts \(E_{PK_D}(Key_{S,D})\) with its private key \(SK_D\) and checks the validity of hashed value. Then node D waits for some time to receive different instances of \(RREQ_{S,D}\) from different routes. Node D then constructs maximum set of node-disjoint paths and composes route reply message \(REP_{D,S}\) for each instance of \(RREQ_{S,D}\) with different \(List_{Route}\).

\[
REP_{D,S} = <ID_S, ID_D, SEQ, List_{Route}, Trust_{Route}, hash_{Key_{S,D}} (ID_S, ID_D, SEQ, List_{Route})>
\]

When each intermediate node \(n_i\) receives \(REP_{D,S}\), it checks its identifier \(ID_i\) in \(List_{Route}\). If not present, the node \(n_i\) drops the packet. Otherwise, it also checks the node identifiers of neighbours before and after its \(ID_i\) in \(List_{Route}\) are in \(N_i\). Then, node \(n_i\) rebroadcasts \(REP_{D,S}\) until it reaches the source node S. Finally, when \(REP_{D,S}\) reaches the source node S, it verifies the hash value of \(hash_{Key_{S,D}} (ID_S, ID_D, SEQ, List_{Route})\). If it is valid, then \(List_{Route}\) will be stored as valid path to reach destination node D. Once all the route replies from node D are received and node-disjoint paths are stored in the routing table, the source node S prioritizes the paths based on \(Trust_{Route}\). If there are ‘k’ node-disjoint paths are present, then weight factors of paths to decide amount of data to be transmitted through paths are decided as follows:

\[
W_i = \frac{Trust_{Route}^i}{\sum_{i=1}^{k} Trust_{Route}^i}
\]

where \(W_i\) is the weight factor of ‘\(i^{th}\)’ route and \(Trust_{Route}^i\) is the \(Trust_{Route}\) value of ‘\(i^{th}\)’ route.

The source node S transmits the data through different multiple node-disjoint paths based on the trust values of routes. Periodically, the node S recalculates the weights of routes according to their dynamic \(Trust_{Route}\) values.

http://www.iaeme.com/IJCET/index.asp 141 editor@iaeme.com
3.3. SDNMR Algorithm

Input: Each node $n_i$ in MANET has:
- a pair of keys $[PK_i, SK_i]$
- unique identifier $ID_i$
- certificate $CERT_i$ issued by certificate authority

/* authenticating one-hop neighbors */
1. Each node $n_i$ broadcasts periodically $Msg_i$
   $<t, ID_i, sig_i(t, ID_i), CERT_i>$
2. Each node $n_i$ builds one-hop neighbour list $N_i$ at time $t$

/* at source node */
3. Source node $S$ issues route request query:
   \[ RREQ_{S,D} = <ID_S, ID_D, SEQ, HopCount_{current}, HopCount_{max}, E_{PK_o}(Key_{S,D}), List_{Route}, List_{Exclude}, Trust_{Route}, List_{NextHop}, hash_{Key_{S,D}}(ID_S, ID_D, SEQ, HopCount_{max})> \]

/* at each intermediate node */
4. Each intermediate node $n_i$ hashes the received route request query packet and stores the hashed value of first query packet in its routing table.
   $hash_{Key_{S,D}}(RREQ_{S,D})$
5. If $hash_{Key_{S,D}}(RREQ_{S,D})$ value already present, then
6. Drop $RREQ_{S,D}$
7. Else update $List_{Route}$, $List_{Exclude}$ and $Trust_{Route}$
8. Increment $HopCount_{current}$ by 1
9. If ($HopCount_{current} == HopCount_{max}$) then
10. Drop $RREQ_{S,D}$
11. Else forward $RREQ_{S,D}$

/* at destination node */
12. For each received $RREQ_{S,D}$, the destination node finds the hashed value as: $hash_{Key_{S,D}}(RREQ_{S,D})$
13. Destination node stores all $RREQ_{S,D}$ with different $hash_{Key_{S,D}}(RREQ_{S,D})$ values
14. Compose and broadcasts route reply message as:
   \[ REP_{D,S} = <ID_S, ID_D, SEQ, List_{Route}, Trust_{Route}, hash_{Key_{S,D}}(ID_S, ID_D, SEQ, List_{Route})> \]
15. Each intermediate node $n_i$ checks $REP_{D,S}$ as:
16. If ($ID_i$ is in $List_{Route}$ or neighbours $ID_i$ before and after its $ID_i$ in $List_{Route}$ are in $N_i$) then
17. Broadcasts $REP_{D,S}$
18. Else drop $REP_{D,S}$
/* at source node */
19. for each received $RREP_{D,S}$, source node finds hashed key value as:
\[ hash_{keys,D}(ID_S, ID_D, SEQ, List_{Route}) \]
20. if \( (hash_{keys,D}(ID_S, ID_D, SEQ, List_{Route})) \) not valid
21. drop $RREP_{D,S}$
22. else store $List_{Route}$ in its routing table.
23. For each $List_{Route}$ in its routing table, source node $S$
periodically calculates route trust value factor as:
\[ W_i = \frac{\sum_{i \in List} Trust_i}{\sum_{i \in List} Trust_i} \]
24. Source node $S$ determines and transmits amount of data
through each $List_{Route}$ according to its $W_i$
25. Repeat steps 23 and 24 until entire data is transmitted.

4. SIMULATION ANALYSIS OF SDNMR PROTOCOL

The performance of proposed protocol SDNMR is analysed using NS2 simulator [48] which
is a discrete-event simulator used widely by networking academic research community
people. The simulated model of MANET with 50 nodes distributed randomly in an area of
1000 m X 1000 m. Node propagation range is 250m and data transmission rate is 2m/s.

Random way point mobility model is considered to simulate the mobility behaviour of
nodes. According to this model, a node randomly selects a destination node and then moves
towards it with a random speed. After reaching the destination node, the node waits for certain
pause time and then again, the node selects another random destination node and moves
towards it with random speed. This way node mobility is simulated according to this model.
In our simulation model, the node pause times are fixed as 0, 5, 10, 20, 30 and 40s. Pause
time 0 means the nodes are continuously moving and pause time 40 means the nodes are
stationary.

In our simulation runs, we selected randomly 10 pairs of source and destination nodes.
The application data to be transmitted from source to destination is generated by traffic
application CBR (Constant Bit Rate) with packet size 512 bytes. The simulation is conducted
for 350s of simulation time. The medium access control protocol used in the simulation is
IEEE 802.11 Distributed Coordination Function (DCF). During the discovery of node-disjoint
multiple paths, we made destination node to wait for 5s to receive distinct route request
messages and reply them. The simulations are run with various traffic scenarios with different
interpacket times and for each scenario, ten movement patterns are considered. Our
simulations used free space radio model.

Since our secure protocol SDNMR is inspired from the previous work [41], [42],
simulation results of SDNMR are compared with that work.

Inspite of many security measures, it is difficult to detect selfish nodes that are dropping
data packets at critical time. These selfish nodes participate in route discovery and become
the part of path but they drop the data packets to save their battery power. Our protocol SDNMR
takes care of such selfish nodes by considering trust values of nodes in the path. Average
throughput of all communicating pairs in MANET is calculated by increasing the number of
misbehaving nodes and the results are shown in Fig. 2. It is observed from the results that
SDNMR performs better than SecMR [41] and protocol [42] because they do not consider selfish node attacks. SecMR is not addressing any kind of data security other than the discovery of secured multiple node-disjoint paths. The protocol [42] discovers trustworthy routes and data is then encrypted and transmitted through paths and no protection for data drop. But our protocol SDNMR is focused in both issues of secure route discovery and dropping of data packets. Hence SDNMR is giving more throughput than others. Similarly, average end-to-end latency is also measured as it is an important metric of network performance and it is shown in Fig.3. SDNMR is better in end-to-end delay compared to other work SecMR and [42]. Usually, there is a trade-off between security overhead and network delay. But our SDNMR is providing security with significant delay since it is using simple trust model and path trust is calculated periodically as the part of route maintenance. In [42], the data is transmitted through multiple paths by encrypting each packet, hence it is taking more time than SDNMR.

Since node mobility is affecting network topology and thereby routing paths, we also measured network throughput with respect to node speed. Fig. 4 shows the result of network throughput with respect to node mobility. SDNMR gives better results than [42] as the route discovery process includes authenticating neighbourhood and also exclude list is used to avoid the nodes that could present in multiple paths. When a node moves away from path, it will be listed in exclude list and thereby path will be modified hence it results in high throughput than [42] where such list is not present.

Another important metric of packet drop percentage is also considered for the performance analysis of SDNMR and the results are shown in Fig. 5. SDNMR has the least percentage of data packet drop compared to SecMR and [42] where packet drop by malicious nodes is not considered.

![Figure 2 Network throughput vs malicious nodes](image1)

![Figure 3 Average Delay vs malicious nodes](image2)

![Figure 4 Average Throughput vs Node Mobility](image3)

![Figure 5 Average Package Drop vs Node Mobility](image4)
5. CONCLUSIONS

Routing security and Data security are two important challenges in MANET research area. This paper proposes a new method SDNMR of providing both routing security and data security making use of on-demand node-disjoint multipath routing scheme where asymmetric cryptography and trust-based security concepts are applied. In SDNMR, a complete set of node-disjoint multiple paths which are authenticated and reliable trusted paths are discovered. Also, node trust value computations involve the remaining battery power level so that energy efficient or selfish node free routes can be established. The amount of data to be transmitted through each path is determined in proportion to route trust value which is computed during route discovery process and route trust value is updated periodically during route maintenance. The node-disjoint loop-free secured multiple paths are discovered using asymmetric cryptography authentication principle and trust-based security model is used to prevent attacks from selfish nodes which may drop data packets during critical times of network operation. The general framework of SDNMR can be experimented with suitable node-authentication scheme during route discovery and it is then combined with any reliable trust-based security model. The simulation results of SDNMR shows the significant performance compared to previous related work.

REFERENCES


Secure Data Transmission through Node-Disjoint on Demand Multipath Routing in MANETs


