*Available online at http://www.ijcrls.com*

*International Journal of Current Research in Life Sciences*
*Vol. 07, No. 02, pp.1212-1218, February, 2018*

**ISSN: 2319-9490**

# RESEARCH ARTICLE

## LST BASED SECURE AND TIME EFFICIENT ROUTING IN MANET

**[*1]Mamta and [2]Raghav Yadav**

[1]Department of Computer Science and IT, Shuats, Allahabad, India
[2]Associate professor Department of Computer Science and IT, Shuats, Allahabad, India

Received 19th December, 2017; Accepted 10th January, 2018; Published Online 28th February, 2018

## ABSTRACT

An ad hoc wireless network is a temporary and dynamic environment where a group of mobile nodes with radio frequency transceivers communicate with each other without the intervention of any centralized administration or established infrastructure. Due to the limited transmission range of each mobile node, communication sessions between two nodes are usually established through a number of intermediate nodes, which are supposed to be willing to cooperate while forwarding the messages they receive to their destination. Unfortunately, some of these intermediate nodes might not be trustworthy and might be malicious, thereby forming a threat to the security and/or confidentiality of the exchanged data between the mobile nodes. This paper proposed a partially distributed dynamic model for security against such misbehaving nodes and ensured secure routing in mobile ad hoc networks and it also proposes to make network time delay efficient. The proposed scheme is partially distributed in the sense that supplementary information is propagated amongst nodes implicitly during route establishment rather than the flooding of explicit packets. This supplementary information (in the form of GMC) is used as a cautionary measure against misbehaviour of a node rather than directly considering the accused node as "misbehaving". Co-operation is induced first, using a dynamic time-out based mechanism that threatens misbehaving nodes by blocking all communications with them in accordance to the severity of their misbehaviour. The timer for which a node is blocked depends upon past communication with that node and the frequency of its misbehaviour locally, i.e., LMC and globally, i.e., GMC. Different weights are assigned to both LMC and GMC for efficacy of system performance. Secondly, a dynamic credit allotment mechanism that reciprocates a node's behaviour by allotting Chips to it is employed. It precisely examines the overall behavior of a node in the network by considering not only its forwarding behaviour with the host node but also supplementary information received regarding its behaviour from other nodes. It was also concluded that if we use least spaning tree for the MANET then the time efficiency has been increased.

***Key words:*** Mobile Ad-hoc Network, Wireless Sensor Node, GMC, LMC, Least Spanning Tree.



**Citation: Mamta and Raghav Yadav, 2018.** "Lst based secure and time efficient routing in manet" *International Journal of Current Research in Life Sciences*, 7, (03), 1212-1218.

## INTRODUCTION

As the importance of computers in our daily life increases, it also sets new demands for connectivity. Wired solutions have been around for a long time but there is increasing demand on working wireless solutions for connecting the Internet, reading and sending E-mail messages, changing information in a meeting and so on. There are solutions to these needs, one being wireless local area network that is based on IEEE 802.11 standard. However, there is increasing need for connectivity in situations where there is no base station (i.e. backbone connection) available (for example two or more PDAs need to be connected), there emerges Ad hoc networks (Perlman, 2000). In Latin, Ad hoc means "for this", further meaning "for this purpose only". This is a good and emblematic description of the idea why Ad hoc networks are needed. They can be set up anywhere without any need for external infrastructure (like wires or base stations). They are often mobile and termed as Mobile Ad hoc Networks (MANET) (Marti *et al*., 2000). MANET is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. The popular IEEE 802.11 "Wi-Fi" protocol is capable of providing Ad hoc network facilities at low level, when no access point is available. However in this case, the nodes are limited to send and receive information but do not route anything across the network. Mobile Ad hoc Networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet. Mobile Ad hoc Networks can turn the dream of getting connected "anywhere at any time" into reality. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places. As an example, imagine a group of people with laptops, in a business meeting at a place where no network services is present. In such a situation their machines can form an Ad hoc network. This is one of the many examples where these networks may possibly

***Corresponding author:*** **Mamta,**
Department of computer science and IT, Shuats, Allahabad, India.

be the best ones to cater the needs of dynamic nature. Mobile Ad hoc Network (MANET) has received much attention due to self-design, self-maintenance, self-organized and cooperative environments. In MANET, all the nodes are mobile nodes and the topology will change rapidly without any predefined infrastructure. Participating nodes can be laptops, palmtops, cell phones etc. Each device can act both as a host and a router to forward packets for other nodes. Here, the mobile devices such as PDAs and laptops are used to route the data packets. In MANET, all the nodes actively discover the topology and the messages are transmitted to the destination over multiple-hop. It uses the wireless channel and asynchronous data transmission through the multiple-hop. The vital characteristics of MANETs are lack of infrastructure, dynamic topology, multi-hop communication and distributed coordination among all the nodes. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or to deploy an infrastructure which is cost effective on a temporary basis. Some applications of Ad hoc networks include students using laptop to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information about situation awareness in a battlefield, and emerging disaster relief after an earthquake or hurricane. Ad hoc networks are created, for example, when a group of people come together and use wireless communication for some computer based collaborative activities; this is also referred to as spontaneous networking. The nodes are free to move randomly and organize themselves arbitrarily, thus the wireless network topology may change rapidly and unpredictably. Such a network may operate in standalone fashion as shown in Figure 1.

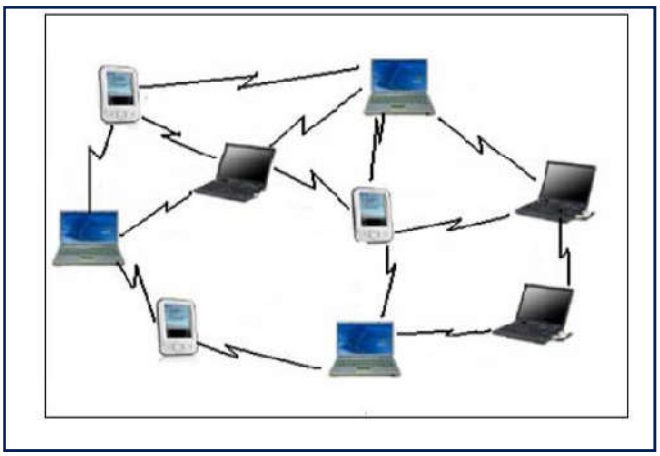


**Fig. 1. MANET Operation**

The main objectives of this paper are to design a dynamic model schemes which provide a partially distributed mechanism and creating a unique blend of both local and global reputation for dealing with misbehaving nodes with time efficient approach.It also study the dynamic model for differential treatments to various misbehaving nodes depending upon the severity of their misbehaviour and evaluate the time efficiency of the MANET.

## Literature Review

The node misbehavior problems in mobile ad hoc network have been studied by many researchers (Perkins, 1994; Buchegger, 2002; Papadimitratos, 2003; Schneier, 1996; Rivest, 1992) and various techniques have been proposed to prevent node misbehavior on data forwarding. These schemes are broadly classified into two categories: detection solutions and preventive solutions. There have been constant efforts made by researchers to increase the security of ad hoc routing protocols. In this section, since our scheme is based upon the anonymous communication paradigms, we will first review related routing algorithms for anonymous communication systems, and then review previous secure ad hoc routing schemes. Anonymous communication in the onion routing protocol. A variety of widely known intrusion techniques may be used to infer the entities' identities, their locations, and/or relationships between communicating entities in a public network. Typical malicious actions may affect the message coding, timing, message volume, flooding, intersection and collusion. Onion Routing (Clausen, 2002) is a communication protocol that is resistance against some of these attacks. It employs a network of Chaum MIXes (Ramanathan, 1996) in order to provide anonymous and secure communications. For data moving backward, from the recipient to the initiator, the process occurs in the reverse order, with the recipient's proxy1194 A. (Papadimitratos, 2002; Imielinski, 1999)/ Computer Communications 28 (2005) 1193–1203breaking the traffic into cells, and successive onion routers encrypting the cells it for the return journey. In the connection termination phase, the anonymous connection established in the connection setup phase is torn down. This involves the removal of encoded next hop information in each onion router making up the connection.

## Finding anonymous paths in current anonymous communication systems

Over the Internet, anonymous systems (Perkins, 1994; Clausen *et al*., 2001; Perlman, 2000) use application level routing to provide anonymity through afixed core set of MIXes, as we described earlier for the Onion Routing protocol. Each host keeps a global view of the network topology, and make anonymous connections through a sequence of MIXes instead of making direct socket connections to other hosts. The authors in (Moy, 1998) used an alternate Onion Routing approach to provide anonymous communications for mobile agents in the JADE environment (Java Adaptive Dynamic Environment). Each JADE multi-agent has several onion agents that provide an anonymous data forwarding service, and at least one onion monitor agent that keeps track of the location of all other onion agents in the system. Onion monitor agents exchange onion agent reach ability information in order to maintain a valid topology of the complete onion agent network. Levien (Perkins, 1999; Johnson *et al*., 2001) developed a monitoring utility that queries MIXes and publishes on a website the average latency and uptime of each MIX over the past 12 days. Recently, Tarzan (Johnson, 2002) and Morph Mix (Perkins *et al*., 2003) have discussed the difficulties of constructing routes in dynamic environments. 3

## Securing ad hoc networks routing protocol

Achieving secure routing in wireless ad hoc networks is a complex task due to the nature of the wireless environment and the lack of predefined infrastructure (Murphy, 2002; Stajano, 1999; Sanzgiri *et al*., 2002). A number of protocols have been developed to add security to routing in ad hoc networks. Papadimitratos and Haas (Zhang, 1998) proposed Secure Routing Protocol (SRP) based on DSR (Papadimitratos, 2002; Perlman, 1988). The protocol assumes the existence of a security association between the source and destination to

validate the integrity of a discovered route. Dahill (Awerbuch *et al*., 2002) proposed the Authenticated Routing for Ad hoc Networks (ARAN) protocol that uses public key cryptography instead of the shared security association used in the SRP (Zhang, 1998). The protocol has an optional second discovery stage that provides non-repudiating route discovery. Yi (Lundberg, 2000) developed a generalized Security-Aware Adhoc Routing (SAR) protocol for discovering routes that meet a certain security criteria. The protocol requires that all nodes that meet a certain criteria share a common secret key. Venkatraman and Agrawal (Raymond, 2000) proposed an approach for enhancing the security of AODV protocol (20), which is based on public key cryptography. In their approach, two systems, External Attack Prevention System (EAPS) and Internal Attack Detection and Correction System (IADCS) were introduced. EAPS works under the assumption of having mutual trust among network nodes while IADC runsby having the mutual suspicion between network nodes.

**System Model**

The number of misbehaving nodes in the network is given by *N* mis. Therefore, the probability of misbehaving nodes in the network is given by:

$$C_{mis} = \frac{N_{mis}}{N} \tag{1}$$

Where *N* is the number of nodes forming the network. A route can be defined as "secure" if none of the nodes forming the route is "misbehaving." Let the average number of hops in a route be *q*. The probability of finding a secure route between source *S*and destination *D* can be given as (Perrig *et al*., 2001):

$$P_{sec}(S,D) = (1 - \frac{Cmis}{N})^{q-1} . \tag{2}$$

To comprehend the impact of the number of misbehaving nodes on the probability of finding a secure route, the value of *q* must be estimated. If the average distance between any two nodes *ni* and *nj* in the network is *d* (*ni, nj*) and the average number of hops in a route is *q*. Then, the average distance between source *S* and destination *D* is given as (Perrig *et al*., 2001):

$$d(S,D) = q * d(n_i, n_j) \tag{3}$$

Let the transmission range of a node extend from point (*xo, yo*) to (*x, y*). Then the radius of the transmission circle of the node can be determined as (Perrig *et al*., 2001):

$$R = \frac{\sqrt{(x-x0)^2+(y-y0)^2}}{2} \tag{4}$$

*Node Density,* the number of nodes per unit of network area, is expressed as:

$$NodeDensity = \frac{N}{A\sqrt{B^2-A^2}} \tag{5}$$

Where A=$\sqrt{(a-a0)^2}$ and B=$\sqrt{(a-a0)^2+(b-b0)^2}$

The average number of nodes *N*avg (*R*) within the transmission circle of a node having range *R* can be expressed as (Imielinski, 1999):

$$N_{nav}(R) = \frac{N}{(a-a0)(b-b0)} \int_0^R 2\pi r dr \tag{6}$$

The probability that all *N*avg (*R*) lie within the circle of radius *r*is determined as:

*F*(*r*) = All *N*avg (*R*) lie within cirle of radius *r,*

$$F(r) = \left(1 - \frac{R^2-r^2}{R^2}\right)^{N_{nav}(R)} \tag{7}$$

The *probability density function* of distance *r* from source *S* is given by:

$$f(r) = N_{nav}(R)\left(\frac{2r}{R^2}\right)\left(1 - \frac{R^2-r^2}{R^2}\right)^{N_{nav}(R)-1} \tag{8}$$

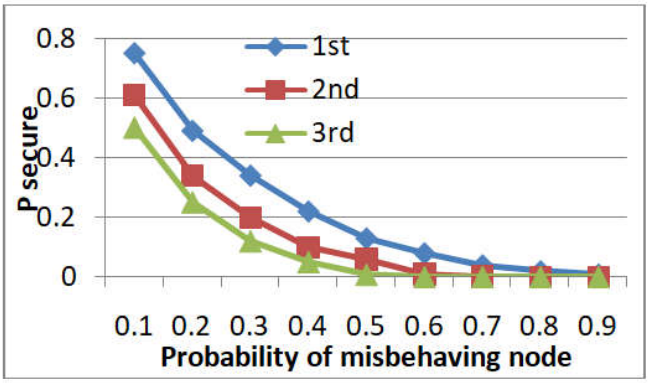



**Fig. 2. Probability of finding a secure route in different cases**

The average distance *d*(*ni, nj*) between any two nodes *ni* and *nj* is:

$$d(n_i, n_j) = \frac{2N_{nav}(R)R}{2N_{nav}(R)R+1} \tag{10}$$

$$q = \frac{d(S,D)}{d(n_i,n_j)} = \frac{(2N_{nav}(R)R+1)\sqrt{(a-a0)^2+(b-b0)^2}}{2N_{nav}(R)R} \tag{11}$$

Finally from equation (2) and (11)

$$P_{sec}(S,D) = (1 - \frac{N_{mis}}{N})^{\frac{(2N_{nav}(R)R+1)\sqrt{(a-a0)^2+(b-b0)^2}}{2N_{nav}(R)R}-1} \tag{12}$$

Fig. 2 illustrates the effect of varying the probability of misbehaving nodes *P*m is on the probability of finding a secure route *PSEC* (*S,D*) in different environments. Three different cases are considered for analyzing the effect of the probability of misbehaving nodes *P*m is on the probability of finding a secure route *PSEC*(*S,D*) between source *S* and destination *D*. For simplicity of discussion, the starting coordinates of the transmission range (*xo, yo*) and that of the network area (*ao, bo*) are taken as (0, 0). The cases are as follows:

**1st Case:** *N* is taken as 200. The coordinates of a node's transmission range (*x, y*) are taken as (*x, x*). The coordinates of the network area are taken as (4*R,* 4*R*), i.e., four times the transmission range.

***2nd*Case:** *N* is taken as 300. The coordinates of a node's transmission range (*x, y*) are taken as (*x, x*). The coordinates of the network area are taken as (6*R,* 6*R*), i.e., six times the transmission range.

**3rdCase**: *N* is taken as 400. The coordinates of a node's transmission range (*x, y*) are taken as (*x, x*). The coordinates of the network area are taken as (10*R,* 10*R*), i.e., ten times the

transmission range. From Fig. 2, it can be observed that the probability of finding a secure route *PSEC*(*S,D*) decreases when the probability of misbehaving nodes *P*m is, in the network increases. It can been seen that the value of *PSEC* (*S,D*) decreases with an increase in network area. The reason is the increase in the average number of hops in the route as the routes become longer. In Case 2, when *P*mis≥0.3, the probability of finding a secure route falls below 50 percent. This low probability of finding a secure route can profoundly deteriorate the network performance. Hence, it is indispensable to provide an efficient mechanism for secure routing in MANETs, which forms the basis of this research.

**Proposed System Model**

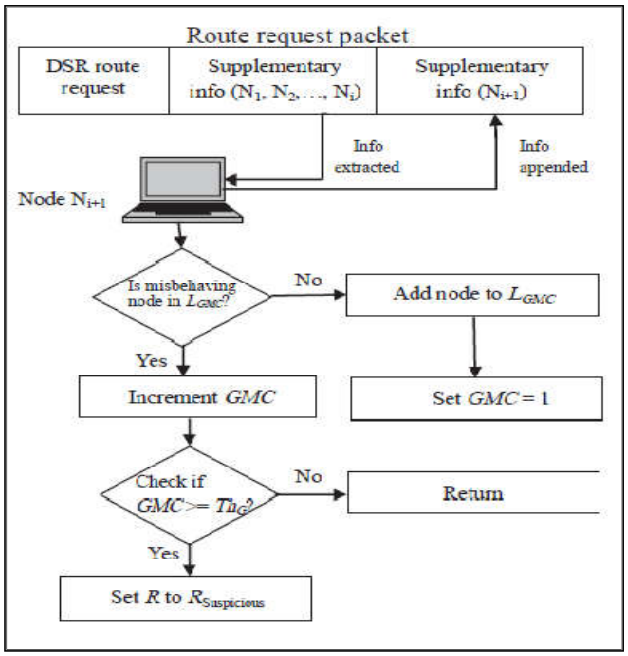
The proposed scheme makes use of the collective information (i.e., local reputation information and supplementary information from other nodes) for detecting and handling routing misbehavior. This information, along with other parameters, is used for dynamic handling of misbehaving nodes according to the severity of their misbehavior. The proposed scheme is partially distributed in the context of information propagation. Information regarding misbehavior is purveyed through a route request packet only when a node must transmit its data, rather than using explicitly generated messages at regular intervals, as in the case of other reputation based schemes. Once a route request packet containing supplementary information reaches the destination node, it will not propagate the route request packet (containing supplementary information) further in the network. Moreover, nodes generating Route Reply using information from their route cache do not broadcast the route request packet (containing supplementary information) any further in the network.

In the local reputation information each node runs an overhearing mechanism for tracking misbehaving nodes in the network. When a host node transfers a packet to its neighbour node, the overhearing mechanism listens to the wireless channel in promiscuous mode to determine if the. The overhearing mechanism monitors the channel for a specified time *TOH*. On overhearing neighbor's effort to forward a packet, it compares the checksum of the sent packet with that of the packet forwarded by the neighbor node. A match found indicates that the packet has been successfully forwarded. If the packet is not forwarded within *TOH*, it is considered to be dropped. Nodes in the network maintain rating *R*ni for each of their neighbor nodes *ni*. The value of rating *R*ni is updated depending upon whether the neighbor has forwarded the packet or not. The rating *R*ni is incremented by a value *Ri* on successful packet forwarding by the neighbor. Conversely, rating *R*ni is decremented by a value *Rd* if the packet is not forwarded within *TOH*. When the rating of node *ni* falls below *R*min i.e., *R*ni≤*R* min, the node is added to the list of misbehaving nodes *L*mis. Hence, each node maintains a local list of nodes that it considers as misbehaving. In the global supplementary information, the Nodes of the network, convey information regarding nodes that they consider to be misbehaving. This supplementary information is communicated to other nodes during route setup in the form of a Dissemination List *LD*. An additional field (of variable length) is added to the DSR route-request (*RREQ*) packet. A node receiving the *RREQ* packet performs two functions. First, it uses the supplementary information contained in the *RREQ* packet to create and maintain a global misbehaving count (*GMC*) list *LGMC*. This list maintains an account of the number of nodes that consider a particular node as misbehaving.

List *LGMC* consists of two fields: *node id* and *GMC*. *Node id* contains the *id* of the node considered as misbehaving. *GMC* indicates the number of nodes that consider the particular node as misbehaving. List *LGMC* provides cautionary information to the host node which it uses to reset the rating of misbehaving nodes contained in List *LGMC*. If the value of *GMC* for a particular node in list *LGMC* is greater than or equal to *ThG*, i.e.,*GMC* ≥*ThG*, then the rating *R*ni of that node is decreased to *R* Suspicious. The value of *R*Suspicious is taken as slightly greater than *R*min for quick detection of its misbehavior. Secondly, it appends its local list of misbehaving nodes *L*mis to list *LD* in the *RREQ* packet before re-broadcasting it in the network. It is to be noted that a node can only be added to list *L*mis through direct observation and not on the basis of supplementary information. This is to avoid the problem of false accusation by a group of misbehaving nodes that may falsely accuse a well behaving node as "misbehaving". Fig. 2 depicts how a node *ni*+1 uses the supplementary information contained in the route request packet to update its list *LGMC*. Algorithm 1 presents the steps involved in the creation and update of list *LGMC*. The worst case complexity of the algorithm is *O*(*nk*), where *n* and *k* are the lengths of lists *LD* and *LGMC* respectively.

The Dynamic Node Blocking (DNB) mechanism is responsible for blocking all communications with nodes that are added to list *L*mis. Communications with misbehaving node *nj* are blocked for only a certain time period *TDNB*(*nj*). When *TDNB*(*nj*) expires, node *nj* is removed from list *L*mis and all communications with it are resumed. The nodes added to list *L*mis are not blocked for an indefinite time for the following reasons. First, a node could be incapable of forwarding packets owing to some kind of failure and that could be misconceived as misbehaving. Such a node could resume its functionality after recovery from the failure. Secondly, misbehaving nodes must be provided an opportunity to concede their misbehavior. However, in the case of continued is behavior, node *nj*can be added back to list *L*mis with further adjustments of *TDNB*(*nj*) according to the severity of itsmis behavior. Timer *TDNB*(*nj*) is dynamic in nature as it depends upon past communication with the misbehaving node *nj*, represented by *F*(*P*(*ni, nj*)*, P*(*nj, ni*)). It also depends upon the frequency of its misbehavior locally, *LMC* and globally, *GMC*. Different weights are assigned to LMC and GMC. *LMC* is given more weight than *GMC* for better performance of the system. In the case of repeated misbehavior, locally and globally, the value of function *G*(*LMC,GMC*) for node *nj* would increase, further increasing timer *TDNB*(*nj*). Moreover, if the node does not participate in packet forwarding, the value of function *F*(*P*(*ni, nj*)*, P*(*nj, ni*)) increases, further extending the timer *TDNB*(*nj*) for node *nj*. Algorithm 2 illustrates how the DNB mechanism calculates the timer value for each misbehaving node *nj*. The complexity of the algorithm is *O*(*c*), where *c* >0. The Dynamic Chips Allotment (DCA) mechanism is deployed at each node in the network for handling of non-participation misbehavior. Nodes maintain are cord of *Chips* (*λ*) for each of their neighbor nodes. *Chips* (*λ*) for a neighbor node *nj* are decremented by node *ni* when node *nj* requests the node *ni* to forward its packets. Conversely, *Chips* (*λ*) for a neighbor node *nj* are incremented by node *ni* when neighbor node *nj* forwards packets of node *ni*. When anynode *ni* receives a forwarding

request by a node *nj*, it first checks the *Chips* ($\lambda$) for node *nj*. The packet is forwarded only if the value of *Chips* ($\lambda$) is not equal to zero. *Chips* ($\lambda$) for each node are initialized to $\lambda o$ to initiate the communications. However, nodes must forward packets for other nodes to maintain their *Chips* ($\lambda$) at other nodes if they wish to transfer their packets through them. *Chips* ($\lambda$) for each node are incremented by a value ($\lambda DCA$) after a fixed time interval, known as DCA Timer *TDCA*. This is for two reasons: First, certain nodes may not have sufficient opportunity to forward packets for other nodes owing to their location in the network (such as peripheral nodes) that may lower their *Chips* ($\lambda$) even when they do not intend to misbehave and are willing to participate in the network functions. Secondly, this is to promote synergy in the network by motivating nodes to behave well for maintaining adequate *Chips* at other nodes to transfer their packets through them. Algorithm 3 illustrates how the DCA mechanism calculates the *Chips* for each node according to its forwarding behaviour and supplementary information received from other nodes.




**Algorithm (Least Spanning Tree)**

- Initialization: $V_1$=Sink, E′=null, and $V_2$=V-$V_1$.
- Select a edge: which has minimum distance from Sink to one cluster-head (suppose is $V_i$), where $V_i$ is directly connected with Sink, then set, $V_1$= {Sink, $V_i$}, E ′= {(Sink, $V_i$)}, $V_2$=$V_2$-$V_1$.
- 3.For each cluster-head $V_k$ in $V_1$ do :select a minimum distance d(k,j),which $V_k$Є$V_1$,$V_j$Є $V_2$ and E′=($V_k$, $V_j$) Є E ,but $V_k$ is not Є E′, then $V_1$=$V_1$Є$V_j$, E′={($V_k$, $V_j$)} Є E′, $V_2$=$V_2$-$V_j$.
- If $V_2$ is empty then end, else go to above

## RESULTS AND DISCUSSION

The simulation results obtained for the proposed scheme (referred to as PDDM) and other existing algorithms. Fig. 4 illustrates the packet success ratio of the proposed scheme (PDDM) and other deployed schemes. The packet success ratio of the proposed scheme is significantly greater than that of the other schemes in the presence of misbehaving nodes. This is a result of the ability of PDDM to handle the misbehaving nodes according to the severity of their misbehavior using local and global information.

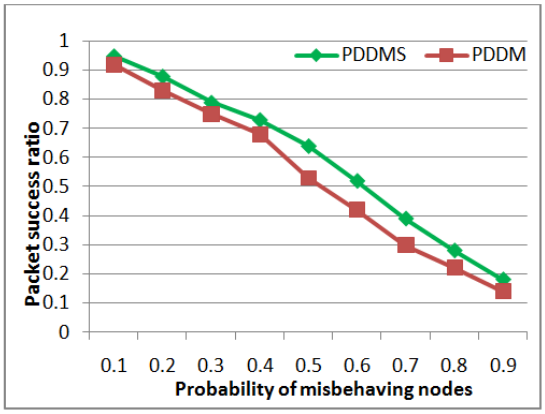



**Fig. 4. Packet success ratio of the proposed scheme and other reputation based schemes**

It can be observed that the packet success ratio decelerates quickly as the probability of misbehaving nodes *P*m is in the network increases. Networks with such high probability of misbehaving nodes are impractical and must be discarded.

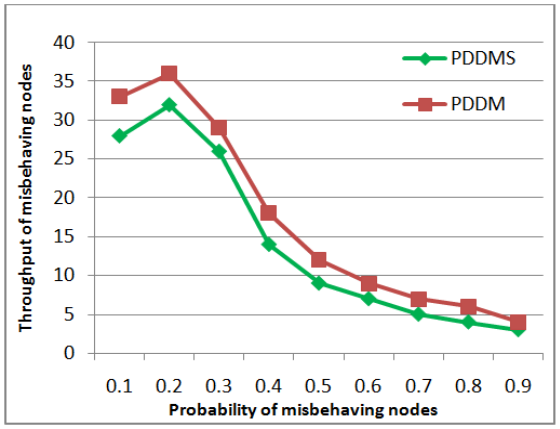



**Fig. 5. Through put of misbehaving nodes in proposed scheme and other reputation based schemes**

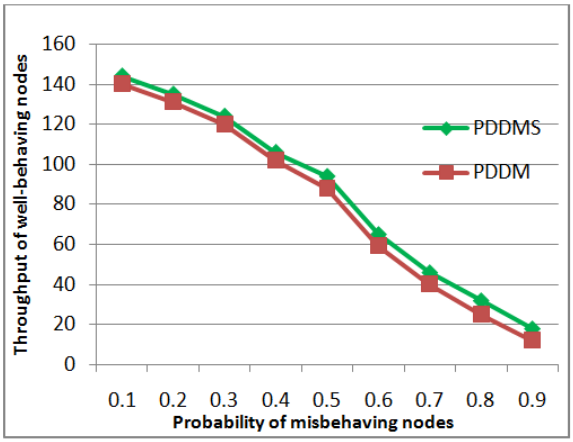



**Fig. 6. Throughput of well-behaving nodes in the proposed scheme and other existing schemes**

Figs. 5 and 6 illustrate the throughput of misbehaving and well-behaving nodes in the proposed scheme (PDDM) along with other reputation based schemes. The throughput of the misbehaving nodes, in the case of PDDM, is less than all other deployed algorithms. The fig. 7 shows that the proposed method based LST gives better throughput compared to without LST method and speed of transmission will be high in this method.

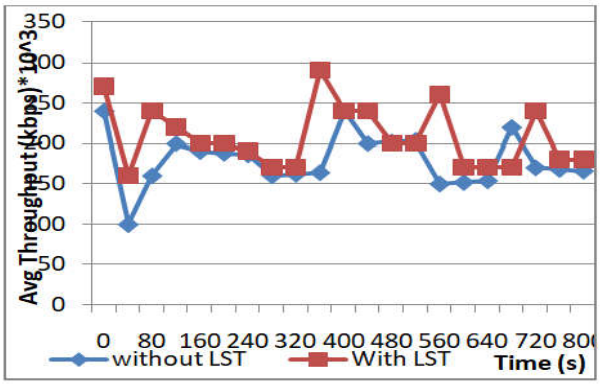



**Fig. 7. Throughput of well-behaving nodes in the proposed scheme and other existing schemes**

Due to implementation MANET it has increased the speed of data transfer due to data compression and fusion process.

## Conclusion

The inherent features of MANETs such as dynamic topology, lack of central administrating authority, and paucity of resources prompt nodes in the network to misbehave. A node may exhibit varying kinds of misbehaviors during its lifetime. This paper proposed a partially distributed dynamic model for security against such misbehaving nodes and ensured secure routing in mobile ad hoc networks. The proposed scheme is par-tially distributed in the sense that supplementary information is propagated amongst nodes implicitly during route establishment rather than the flooding of explicit packets. This supplementary information (in the form of *GMC*) is used as a cautionary measure against misbehavior of a node rather than directly considering the accused node as "misbehaving". Co-operation is induced first, using a dynamic time-out based mechanism that threatens misbehaving nodes by blocking all communications with them in accordance to the severity of their misbehavior. The timer for which a node is blocked depends upon past communication with that node and the frequency of its misbehaviorlocally, i.e., *LMC* and globally, i.e., *GMC*. Different weights are assigned to both *LMC* and *GMC* for efficacy of system performance. Secondly, a dynamic credit allotment mechanism that reciprocatesa node's behavior by allotting *Chips* to it is employed. It precisely examines the overall behavior of a node in the network by considering not only its forwarding behavior with the hostnode but also supplementary information received regarding its behavior from other nodes. It was also concluded that if we use least spaning tree for the MANET then the time efficiency has been increased.

## REFERENCES


Awerbuch, B., Holmer, D., Nita-Rotaru, C. and Rubens, H. 2002. "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," *WISE'02*, Atlanta, Georgia, September, pp. 21-30.

Buchegger, S. and Le Boudec, J.Y. 2002. "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks)," *Proc. 3rd Symp. Mobile Ad hoc Networking and Computing (MobiHoc 2002)*, ACM Press, pp. 226-236.

Capkun, S. and Hubaux, J.P. 2003. "BISS: Building Secure Routing out of an Incomplete Set of Security Associations," *Proc. ACM Workshop on Wireless Security*, ACM Press, pp. 21-29.

Clausen, T., Hansen, G., Christensen, L. and Behrmann, G. 2001. "The Optimized Link State Routing Protocol – Evaluation Through Experiments and Simulation," *Proc. 4th Int'l. Symp. Wireless Personal Multimedia Communications*, Aalborg, Denmark, September, 6 pp.

Clausen, T., Jacquet, P. and Viennot, L. 2002. "Comparative Study of Routing Protocols for Mobile Ad hoc Networks," *Med-Hoc-Net'02*, Sardegna, Italy, September, 10 pp.

Eastlake, D. and Jones, P. 2001. "US Secure Hash Algorithm 1 (SHA1)," RFC 3174, September.

Hu, Y.C., Johnson, D.B. and Perrig, A. 2002. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," *Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications*, Callicoon, NY, June, pp. 3-13.

Hu, Y.C., Perrig, A. and Johnson, D.B. 2002. "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," *Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02)*, Atlanta, Georgia, September, pp. 12-23.

Hu, Y.C., Perrig, A., and Johnson, D.B. 2003. "Packet Leashes: A DefenseAgainst Wormhole Attacks in Wireless Ad hoc Networks," *Proc. 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom'03)*, San Francisco, CA, April.

Imielinski, T. and Navas, J.C. 1999. "GPS-based Geographic Addressing, Routing, and Resource Discovery," *Communications of the ACM*, vol. 42, no. 4, April, pp. 86-92.

Johnson, D.B., Maltz, D.A., and Broch, J. 2001. "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," *Ad Hoc Networking*, C.E. Perkins, Ed., Addison-Wesley, 139-172.

Johnson, D.B., Maltz, D.A., Hu, Y.C. and Jetcheva, J.G. 2002. "The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR)," Internet Draft, draft-ietf-manet-dsr-07.txt, February.

Lundberg, J. "Routing Security in Ad hoc Networks,"http://citeseer.nj.nec.com/400961.html

Marti, S., Giuli, T.J., Lai, K. and Baker, M. 2000. "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," *Proc. 6th Annual ACM/IEEE Int'l. Conf. Mobile Computing and Networking (Mobicom'00)*, Boston, Massachusetts, August, pp. 255-265.

Moy, J. 1998. "Open Shortest Path First (OSPF) Version 2," RFC 2328, April.

Murphy, S. 2002. "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, October.

Papadimitratos, P. and Haas, Z.J. 2003. "Secure Link State Routing for Mobile Ad hoc Networks," *Proc. IEEE Workshop on Security and Assurance in Ad hoc Networks*, IEEE Press, pp. 27-31.

Papadimitratos, P. and Haas, Z.J. 2002. "Secure Routing for Mobile Ad hoc Networks," *Proc. Communication Networks and Distributed Systems, Modeling and Simulation Conf. (CNDS'02)*, San Antonio, Texas, January, pp. 27-31.

Papadimitratos, P. and Haas, Z.J. 2002. "Securing the Internet Routing Infrastructure," *IEEE Communications*, vol. 10, no. 40, October, pp. 60-68.

Perkins, C.E and E.M. Royer, "Ad hoc On-Demand Distance Vector Routing," *Proc. 2nd IEEE Workshop Mobile*

*Computing Systems and Applications*, New Orleans, LA, February 1999, pp. 90-100.

Perkins, C.E. and Bhagwat, P. 1994. "Highly Dynamic Destination-Sequenced Distance-Vector (DSDV) for Mobile Computers," *Proc. ACM Conf. Communications Architectures and Protocols (SIGCOMM'94)*, London, UK, August, pp. 234-244.

Perkins, C.E., Royer, E.M. and Das, S. 2003."Ad hoc On-demand Distance Vector (AODV)," RFC 3561, July.

Perlman, R. 2000. *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols,* Addison-Wesley, Reading, MA, 2000.

Perlman, R. 1988. "Network Layer Protocols with Byzantine Robustness," Ph.D. Dissertation, MIT/LCS/TR-429, MIT, October.

Perrig, A., Canetti, R., Song, D. and Tygar, J.D. 2001. "Efficient and Secure Source Authentication for Multicast," *Proc. Symp. Network and Distributed Systems Security (NDSS'01)*, San Diego, California, February, pp. 35-46.

Ramanathan, S. and Steenstrup, M. 1996. "A Survey of Routing Techniques for Mobile Communications Networks," *Mobile Networks And Applications*, vol. 2, no. 1, October, pp. 89-104.

Raymond, J.F. 2000. "Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems," *Proc. Workshop on Design Issues in Anonymity and Unobservability*, Berkeley, CA, July, pp. 7-26.

Rivest, R. 1992. "The MD5 Message-Digest Algorithm," RFC 1321, April.

Royer, E.M. and Toh, C.K. 1999. "A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks," *IEEE Personal Communications*, vol. 2, no. 6, April, pp. 46-55.

Sanzgiri, K., Dahill, B., Levine, B.N., Shields C. and Royer, E.M. 2002. "A Secure Routing Protocol for Ad hoc Networks", *Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02)*, IEEE Press, pp. 78-87.

Schneier, B. 1996. *Applied Cryptography – Protocols, Algorithms and Source Code in C*, 2nd Ed., John Wiley & Sons, Inc..

Stajano, F. and Anderson, R. 1999. "The Resurrecting Duckling: Security Issues for Ad hoc Wireless Networks," *Proc. 7th Int'l. Workshop on Security Protocols*, Cambridge, UK, April, pp. 172-194.

Toner, S. and D. O'Mahony, "Self-Organising Node Address Management in Ad hoc Networks," *Personal Wireless Communications, IFIP-TC6 8th Int'l. Conf. (PWC 2003)*, 2003, pp. 476-483.

Yi, S., Naldurg, P. and Kravets, R. 2001. "Security-Aware Ad hoc Routing for Wireless Networks," *Proc. 2nd ACM Symp. Mobile Ad hoc Networking and Computing (Mobihoc'01)*, Long Beach, CA, October, pp. 299-302.

Zhang, K. 1998. "Efficient Protocols for Signing Routing Messages," *Proc. Symp. Network and Distributed Systems Security (NDSS'98)*, San Diego, CA, March, pp. 29-35.

Zhou, L. and Haas, Z.J. 1999. "Securing Ad hoc Networks," *IEEE Network Magazine*, vol. 6, no. 13, November/December, pp. 24-30.

*******