A relationship-based approach for energy aware secure routing in MANETs

M.V. Rathnamma*

Jawaharlal Nehru Technological University Anantapuramu (JNTUA),
Anantapuramu 515002, Andhra Pradesh, India
Email: mvrathnamma@gmail.com
*Corresponding author

P. Chenna Reddy

Department of CSE,
JNTUCEP, Pulivendula, Kadapa,
Andhra Pradesh, India
Email: pcreddy1@rediffmail.com

Abstract: Secure routing is one of the major issues which is affecting the widespread use of MANETs. To address this issue several methodologies have been proposed and some of them were able to achieve a considerable amount of success but with a considerable amount of computational overhead. In this paper, we propose a new secure routing mechanism for MANETS. This mechanism uses trust-based method to establish secure routes. It is a family relationship-based approach in which security is established by considering certain parameters which can be used to determine the ingenuity of the nodes. It also considers the parameters like energy consumption and signal strength of the node. The proposed method does not use any protocol specific parameter and thus can be used over any on demand routing protocol like AODV or DSR. As components of MANETs have several resource constraints, this paper aims at providing an improved AODV protocol called secure family-based routing protocol (SFRP) with reduced resource consumption and security enabled.

Keywords: mobile ad hoc network; MANETs; family relationship-based approach; trust, secure routing.

Reference to this paper should be made as follows: Rathnamma, M.V. and Reddy, P.C. (2016) 'A relationship-based approach for energy aware secure routing in MANETs', *Int. J. Smart Grid and Green Communications*, Vol. 1, No. 1, pp.87–101.

Biographical notes: M.V Rathnamma obtained his Master's in Computer Science Engineering from JNTUA, Anantapuramu. He is currently pursuing his PhD degree in JNTUA, Anantapuramu, and while also working as an Assistant Professor in the Department of Computer Science Engineering, KSRM Engineering College, Kadapa (District), Andhra Pradesh. His areas of interest include computer networks, MANETS, bio-inspired networks and other latest trends in technology. He has more than six years of experience in teaching and research in the area of computer science and engineering.

P. Chenna Reddy is working as a Professor in the Department of Computer Science and Engineering, JNTUA College of Engineering, Pulivendula, Kadapa (district), AP, India. He completed his MTech in Computer Science

and Engineering from Bits Pilani and PhD in Computer Networks from JNTUA University, Anantapuramu. His areas of interest include computer networks and mobile computing. He has 15 years of teaching experience.

1 Introduction

A mobile ad hoc network (MANET) is a set or collection of components called nodes that can be connected to each other through a wireless medium (Deng et al., 2002). These nodes can send and receive data if they are connected to each other and are dynamic in nature. The nodes are self-organising and independent in nature with no central administrator controlling the network. In MANET's the nodes may act as hosts as well as routers. Depending upon the source and destination nodes they change their role. If a node is in between source and destination and falls on their route then that node acts as a router and this node is called as intermediate node. A source or a destination node always acts as a host. There are frequent disconnections or link breakages in this network, which results in constantly changing topology (Razzaque et al., 2008). The nodes within a particular radio range can communicate with each other directly and if the nodes are not in the communication range they the communicate using multihop routing. Due to the above mentioned properties these nodes are susceptible to several attacks and thus securing of MANET's is a prime issue.

Till now several security methods have been proposed, but none of them makes a good trade-off between security and performance (Razak et al., 2004). A good security mechanism is the one which maintains the performance with considerable amount of security. As the mobile units, mostly have less processing capability, having complex cryptographic computations is not suitable. In this paper, we have proposed a security method which is based on trust value. The paper is divided into seven sections: Section 2 explains Secure routing in MANET's, Attacks in MANETs are elaborated in Section 3, some of the important secure routing protocols are explained in Section 4, proposed design is explained in Section 5 with advantages in Section 6 and conclusion and future work in Section 7.

2 Secure routing

MANETs do not need an inbuilt network infrastructure and they work in a decentralised mode without any central authority to control. As it uses a wireless communication medium it gives a greater flexibility to the nodes. Each node can communicate directly with all other nodes, which fall under the radio range of the node. Data can be sent and received. If a sender and receiver are not within the radio range of each other still they can communicate with each other by sender creating a hop by hop route to the destination through other nodes available in its radio range. Here the sender and the receiver act as the host and all the intermediate nodes act as routers. As this is a decentralised system the smooth functioning of system depends on the cooperation between the nodes. These nodes need to have a certain level of reliability and cooperation so that data transmission is possible without any data loss (Deng et al., 2002). Thus mutual trust becomes an important factor which eventually determines the ingenuity of the network. Infrastructure less environment also has its take on security because of which fixed topology cannot be maintained and the structure of the network keeps changing continuously.

The wireless medium offers ease of communication at the cost of security. As such the data is not secure and one cannot be sure that the data will reach the intended destination node. The security in MANETS comprises of two components: providing security to the data while it is passing through the medium and passing the data to the destination through the route which consists of reliable nodes which can assure the successful transfer of data through them.

As the medium is wireless the data are susceptible to several attacks. The attacks can be passive or active. Passive attacks are the attacks which do not touch the information transmission, but can listen, capture and use the information without disrupting the transmission. The attacks such as eavesdropping and traffic analysis come under this category. These passive attacks are usually difficult to detect as the data remains unmodified. Detecting the passive attack is more difficult in wireless environments because anybody within the vicinity can listen and capture the data.

There is another category called as active attack. Here the data being transmitted is affected. The user is able to use the data and can modify the data. This attack is comparatively easy to detect than the passive attacks. All these attacks are pertaining to data transmission through the medium. There are several approaches to avoid these attacks. Cryptographic mechanisms like simple encryption, public key cryptography and digital certificate. But due to low battery power and less computational capability and most importantly the absence of centralised authority these mechanisms are difficult to implement.

Apart from providing security of the data in the medium, establishing a secured path which consists of reliable nodes is another issue. While routing, the nodes which are part of the route should be reliable. One should be able to transfer the data to the destination node without any data loss. But this is possible only when all the nodes in the network are reliable. The nodes which are unreliable are called as malicious nodes.

There are several attacks possible due to the malicious nodes. These are either due to external attack or internal attack. External attack is the attack on the network, which is due to the nodes which are not allowed to participate in the network (Razak et al., 2004). Internal attack is the attack which is due to the nodes which are part of the active network. The internal attack affects the network to a greater extent and internal attacks are easy to accomplish as they are initiated by an insider who is a part of the network. Thus, before sending the data to the other nodes sender should ensure that it is reliable.

For establishing this reliability there are two approaches: cryptography-based approach and trust-based approach. Cryptography-based approaches involve the use of cryptographic mechanisms such as public key infrastructure (PKI), certificate authentication, digital signature etc. Another approach is the trust-based approach. This mechanism wholly concentrates on establishing trust among the nodes. The cryptographic mechanisms ensure the security of data, but at the cost of high computation and considerable amount of battery consumption. These mechanisms, though popular are not best suited for MANETs as these traditional cryptographic mechanisms are not efficient in detecting any internal or external node attack (Yan et al., 2008). Moreover, the performance of the network reduces. This is the prime reason why trust-based methods is more prevalent and sought after. Hence there is a need for another approach which will ensure considerable amount of security with a minimum effect on performance. Hence we go for trust-based approach. The trust-based mechanisms are usually less computational intensive and do not need a centralised control for its operation. Trust-based mechanism is aimed at decentralised systems.

3 Attacks in MANETs

- *Black hole attack (Al-Shurman et al., 2004)*

  The black hole attack is due a compromised node inside a network. These compromised nodes tries to get the packets from the neighbouring nodes by claiming themselves as reliable nodes which can forward the packet successfully. Thus, the other nodes which seek transmission of data through a better node (having shortest route or reliable route) send the packet to the malicious node. This malicious node in turn, either drops the packets or performs a DoS attack.

- *Worm hole attack (Hu et al., 2006)*

  Wormhole attack is similar to black hole attack, but here two nodes are involved, usually one is internal node and another one is external node. The internal node pretending to be a trusted node advertises for packets through neighbours. This malicious node receives the packets and transfers the packets to another node which usually does not belong to the network (external node) by creating a tunnel. This node which receives the packets, drops the packets, performs DoS attacks or misuses the packets. This attack eventually causes a heavy packet loss.

- *Sleep deprivation (Razak et al., 2004)*

  Sleep deprivation attack is targeted towards a genuine node. This attack tries to reduce the resource capacity of a node, i.e., it mainly tries to drain the energy of the targeted node unnecessarily. Here the malicious node or attacker might send bogus or false messages which are not genuine. The recipient in turn will process those requests and thus its energy is wasted.

- *Gray hole*

  The gray hole attack is similar to black hole attack, but here packets are dropped selectively. This attack is comparatively difficult to detect than a black hole attack due to its selective dropping nature.

- *Rushing attack*

  In rushing attack the attacker node quickly forwards its packets to the next node in order to gain access in the root discovery process (Nandy and Roy, 2011). Thus, by doing so the attacker exploits the property of duplicate suppression wherein the only initial requests for route discovery are considered and the following route discovery packets of other nodes are discarded. This attack can cause denial of service (Hu et al., 2003).

- *Table overflows attack*

  The attacker tries to create several non-existent routes and tries to fill the routing table of the other nodes. This process continues and eventually the affected node is not able to create any new routes as the routing table gets filled. The table overflow attack usually affects proactive protocols as these protocols update their routing table before routing (Wu et al., 2008; Huang and Lee, 2004).

- *Routing table poisoning (Wu et al., 2008)*

  In this attack the malicious nodes send false routing information to other nodes, resulting in an incorrect interpretation of routes which leads to inefficient routing. This attack is different from routing table overflow attack where the node is not able to create new routes.

4 Secure routing protocols

There are several secure routing protocols proposed based on different security aspects, which are discussed below:

- *Authenticated Routing for Ad hoc Networks (ARAN) (Sanzgiri et al., 2002)*

  ARAN is an on demand routing protocol, which uses certificates to provide security. ARAN follows two step processes: the first is a preliminary certification process and the next step is a route instantiation process. This provides end to end authentication. ARAN uses a trusted certificate server whose public key is known to all valid nodes. Here the routes are activated and deactivated based on traffic flowing through the route.

- *Ariadne (Hu et al., 2002)*

  Ariadne is a secure on-demand routing protocol. Ariadne uses TESLA broadcast authentication protocol for authenticating routing messages. TESLA uses a single message authentication code for authenticating broadcast messages. Ariadne prevents attackers or compromised nodes from attacking the other nodes which are not malicious and it also protects the routes which consist of reliable nodes.

- *Security aware ad hoc routing protocol (SAR)*

  This security protocol has a different ad hoc discovery pattern in which the security attributes are considered as parameters. Here security is considered as a negotiable metric which improves the relevance of route discovered by ad hoc routing protocols. This protocol allows the user to select the behaviour according to the level of protection available (Yi et al., 2001).

- *AODV-SEC (Eichler and Roman, 2006)*

  This protocol is based on ad-hoc on-demand distance vector routing (AODV) protocol. This protocol is primarily based on certificates and PKIs. Here an additional certificate called m-Cert in used. Here public key cryptography is used as a centralised trust anchor.

- *Watchdog*

  The watchdog is a method which is used to identify malicious node. Here the node overhears or listens to its neighbour while routing the data in the promiscuous mode. It checks whether the neighbour is correctly forwarding the data or not. If the neighbouring node is found to drop the data, then that node is considered as malicious (Pakzad and Rafsanjani, 2011).

- *Pathrater*

  Pathrater is a method to detect malicious node. Pathrater uses path-metric. The pathrater selects the path with highest path metric value which corresponds to the shortest route and avoids choosing misbehaving nodes. The path metric can be calculated based on node rating and link reliability. It is an extension to DSR (Pakzad and Rafsanjani, 2011).

- *Patwardhan intrusion detection system (Patwardhan et al., 2005)*

  Patwardhan secure routing uses public key signatures for securing the packets. It also has an intrusion detection system which works in promiscuous mode and listens to the neighbouring packets to detect the malicious nodes.

5 Trust management scheme

In this paper, we propose a new mechanism with a protocol called SFRP to secure routing over MANETs which is based on AODV. This mechanism uses the trust as its base to secure a route. Here we are also considering the energy consumption of each node between transmit and receiving of packets in the network. In Bergamo et al. (2004) an energy control mechanism has been planned as a path to ameliorate the energy efficiency of routing algorithms in ad hoc networks. Each node in the network estimates the power necessary to reach its own neighbours, and this power estimate is used for tuning the transmission power.

There are certain parameters used in these mechanisms which are described below and thereafter a step by step description of the method is given.

This is a security model that works over an existing protocol such as AODV. The nodes are divided into four components i.e., they are given four levels of privileges.

1. *Visitor node*

   This node is the least trusted node. This is the default privilege given to a node which enters the network. This node cannot participate in network routing activities. It can only receive or send messages, but does not have the privilege for routing the packets through it until and unless the trust is calculated and it is upgraded as a child node. This is the first level.

2. *Child node*

   The child node has a higher privilege than the visitor node. The child can send and receive messages and can take part in the routing process. It can give trust value to other nodes.

3 *Parent node*

The parent node has a higher privilege than the child node. This node can also give trust value to all other nodes. The parent node can upgrade a child node as a parent node.

4 *Grandparent node*

The grandparent node has the highest privilege. The grandparent node can upgrade a parent node to a grandparent. This node has the highest privilege. Grandparent is given more importance while calculating trust. This has the highest level.

5.1 Trust calculation

There are three trust values calculated, initial trust, behavioural trust and calculated trust. All the trust values lie between 0 and 1. To maintain the trust values between 0 and 1 we use convex hull methodology.

1 *Initial trust*

Initially, all the nodes will be considered as equal and assigns the fixed Initial trust value as 0.5. So if the trust is calculated for the first time, that would be considered as 0.5.

2 *Behavioural trust*

The behavioural trust value is calculated based on the behaviour of the node. There are several parameters considered for behavioural trust:

a *Ratio of packets sent to, received*

This is the ratio between the number of packets sent to a node and the number of packets received. This always lies between 0 and 1 (while packet forwarding).

b *Previous trust*

This is latest trust value of the node that was calculated. Thus the trust value which was obtained in the previous iteration.

c *Trust rating*

The ratio of number of successful trust predictions to the number of total trust predictions. Behavioural trust is calculated using different parameters for different privilege level. For visitor node only first parameter is considered (ratio of sending and received packets), whereas for the child node first two are considered. For the parent node all the three are considered.

3 *Neighbour trust*

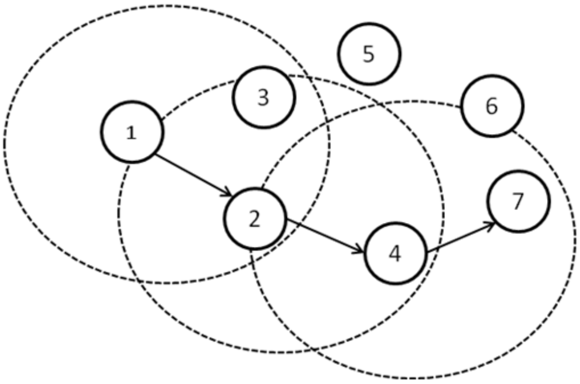
This trust is calculated by the neighbours. The node will approach all the neighbours for the trust value of a node. The neighbours will send the trust value which will range from 0 to 1. All the received values are combined using convex hull set methodology. Here average of all the trust values provided by the mutual neighbours is calculated (if all the mutual neighbours are a child or parent) and the resultant is considered as trust value. If mutual neighbours consist of any grandparent then Preference is given to the node by giving more weight age to its truest value.

4 *Final trust value*

Final trust value is the average of all the three trust values (when the initial value is considered, i.e., for visitor node) or the average of two trust values if the initial value is not considered (non-visitor node).

Consider the following topology:

Figure 1 Secure routing mechanism



This algorithm will work over an existing on demand protocol. Thus, each time when the route is established the trust value is calculated. Here the route is to be established between the nodes 1 and 7 which is shown in Figure 1.

- *Step1*

  In the first step the initial trust value, the battery power and the signal strength are checked for the node 2 by node 1 (assuming node 2 to be the choice of protocol). If the initial trust value is less than the threshold and the signal strength and battery power of node (node 2) is less than 0.5 then the node is considered unfit and is not considered for routing. If the value of the trust is less than the threshold then it is termed as malicious and subsequently it is notified to all the neighbours by updating the value. And if the value of signal strength or battery power is less than 0.5 then no action is taken but it is not considered for routing.

  After this step if the node is found to be unfit for routing then that node is discarded and the route discovery process is again started from the previous level. Here the discarded node is not considered malicious as its declaration of unfitness is because of less resources and not because of trust value

- *Step 2*

  If the node (node 2) successfully clears the first process, then the behavioural trust is calculated for node 2. As mentioned above, the behavioural trust consists of several parameters and according to these parameters the behavioural trust is calculated. Since we are using convex hull set the resultant trust value would lie between 0 and 1. The behavioural trust parameters would vary for each privilege level (1–4 i.e., from visitor to grandparent in order). For a visitor node only one parameter is considered and for the child nodes two parameters are considered, whereas for parent and grandparent nodes different parameters are considered.

If the node is a visitor node then,

$$BT = rs \tag{1}$$

If the node is a child node then,

$$BT = \frac{1}{2}(rs + pt) \tag{2}$$

If the node is a parent or a grandparent then

$$BT = \frac{1}{3(rs + pt + tr)} \tag{3}$$

where *BT* denotes the behavioural trust, *rs* denotes the send/receive packet ratio, *pt* denotes the previous trust and *tr* denotes the trust rating. All the above mentioned values only lie between 0 and 1 including 0 and 1.

- *Step 3*

  After this step the neighbouring node trust is calculated. For calculating neighbouring node trust, the neighbouring nodes of node 1 are considered (as in the present case node 1 is the sender). If the neighbouring nodes of the current node are mutual neighbours of the other node (node 2). Due to different privileges the neighbour trust calculation mechanism is different for grandparent and other nodes. If the neighbouring node is a parent or a child then the trust value of the other node is calculated as follows:

$$NT = \frac{1}{2}\sum_{i=1}^{n} NT_i \tag{4}$$

  where *NT* is the trust of the i^{th} mutual neighbour, *n* is the number of mutual neighbours and the above formula is used when all the nodes are either child or parent or a collection of both.

  If the mutual neighbours consist of grandparents, then the following formula is used for calculating the neighbour trust:

$$NT = \frac{1}{n_1 + 2n_2}\sum_{i=1}^{n} NT_i + \frac{2}{n_1 + 2n_2}\sum_{i=1}^{n} NT_i^* \tag{5}$$

  where n_1 is the number of mutual neighbours, n_2 is the number of mutual neighbours (grandparents), NT_i^* is the trust of the i^{th} mutual neighbour.

- *Step4*

  In this step the final trust value is calculated. The final trust value is an even combination of the initial trust, behavioural and neighbour trust; this is when the initial trust is considered. When a visitor is upgraded to a child node the initial trust value is discarded and only the other two values of the trust values are calculated.

For calculating final trust the following formula is used: (initial trust, i.e., for a visitor node)

$$FT = \frac{1}{3}(IT + BT + NT) \tag{6}$$

For calculating the trust value the following formula is used: (non-visitor node)

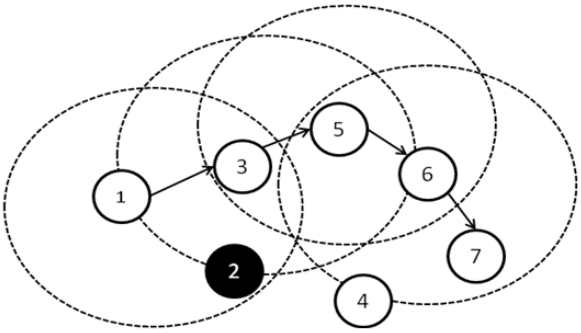
$$FT = \frac{1}{2}(BT + NT) \tag{7}$$

where *FT* is the final trust, *BT* is the behaviour trust, *NT* is the neighbour trust and *IT* is the initial trust.

5.2 Detection of malicious node

Consider the same topology, but here node 2 is malicious. If a node is found to be malicious then the privilege of the node is immediately reduced to the visitor level and the trust value is assigned below the threshold (the final trust value which was calculated in the previous step). Suppose here node 2 is found to be malicious then the final trust value that would have been calculated in the previous step would have been less than the threshold (thr_mal) and as immediate effect, this would be informed to the neighbours and the node would be downgraded to the visitor level with initial trust equal to the malicious trust calculated which is shown in Figure 2.

Figure 2 Malicious node

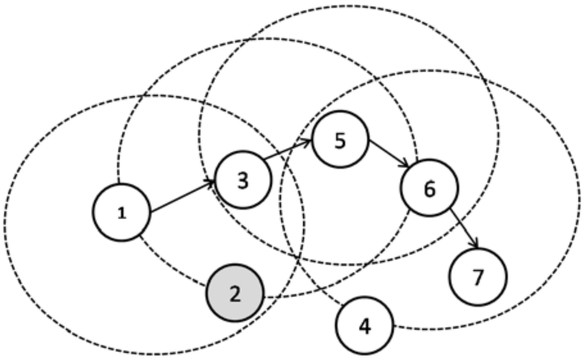


Now that if node 2 is found to be malicious, the node is discarded from the route discovery process, and subsequently the other node in the vicinity is chosen as the next node (choice of the protocol) and the process of route establishment will continue.

5.3 Detection of unfit node

This is another case where the node's battery power or the signal strength is less than 0.5. If this is the case, then the node is discarded from the route discovery process. But the node is not considered as malicious. It is just termed unfit and the privilege and trust value of the node is restored. As the signal strength of a node keeps fluctuating the trust value cannot be dependent on it. The node has a fair chance of coming back to normal stature which is shown in Figure 3.

Figure 3 Unfit node



If the battery power is found to be low, then the power source can be replaced which would ensure that the node can function normally. Thus, here also the trust value should not be changed as the battery power and trust are unrelated.

If the above mentioned problem is encountered, the route discovery process discards the node and proceeds further and choose another node (according to the underlying protocol), and the route is established between the source and destination.

5.4 Trust table

To maintain all the trust values a trust table is maintained. This trust table is maintained by each node. This consists of fields node id, privilege level, battery level, signal strength, behaviour trust, neighbour and final trust, and malicious or not.

Table 1 Sample trust table

Node id	*1*	*5*
Battery	0.7	0.4
Signal	0.84	0.5
BT	0.98	0.9
NT	0.96	0.8
FT	0.97	0.75
Privilege	4	3

6 Results and analysis

This section explains the complete evaluation methodology along with simulation environment and network scenario. This simulation was performed using network simulator, and delivery ratio, delay, routing over head calculated for multiple sets of nodes. We have taken varying malicious nodes from 5 to 25 with different geographical areas.

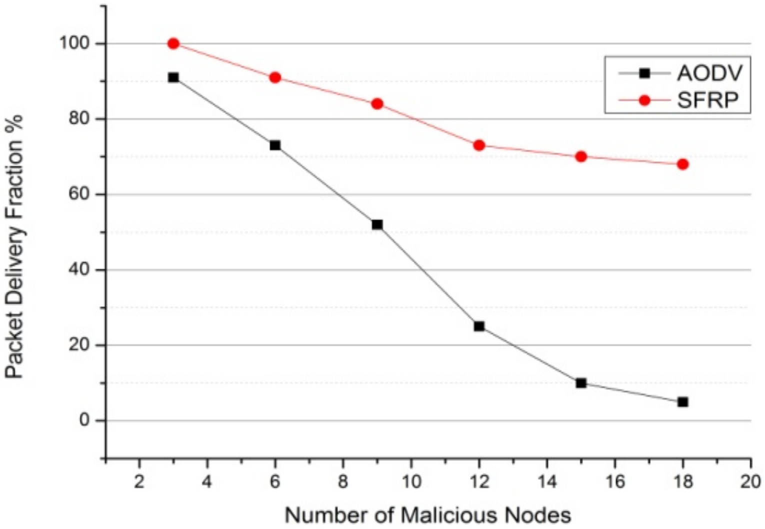
The advantages of this method are: it uses trust-based mechanism which does not involve extensive manipulations. The trust calculation here is using simple mathematical formulas which at the maximum calculate the average of numbers. It is not dependent on any central authority and is wholly distributive in nature. It is a generic approach which would work over any on demand protocol. It is not dependent on protocol specific parameters and hence can be added as a trusted module and slight modifications can be done on it to improve results if necessary. As it is continuous trust calculation the trust value is continuously updated.

Table 2 Simulation parameters

Simulation parameters	*Value*
Number of nodes	150 to 200
Geographical area	300 × 300 sqm
Packet size	512 bytes
Traffic type	CBR
Malicious nodes	5 to 20
Mobility model	Random way point
Pause time	20 s
Simulation time	100 s

The increasing state of number of malicious nodes in the network will degrade the network efficiency and results in the poor performance of network. The proposed approach SFRP can efficiently evaluate the secure trust-based routing with AODV and obtains the maximum accurate detection level of malicious nodes with increasing node capacity.

Figure 4 Packet delivery fraction vs. malicious nodes (see online version for colours)



The packet delivery fraction is more in the improved AODV with trust called, SFRP giving better results than the normal AODV approach. The throughput percentage is calculated by applying different attacks on nodes and got improved results than normal and black hole attack. SFRP is giving the satisfactory results, and avoids black hole and warm hole attacks.

Figure 5 Throughput with time interval (see online version for colours)

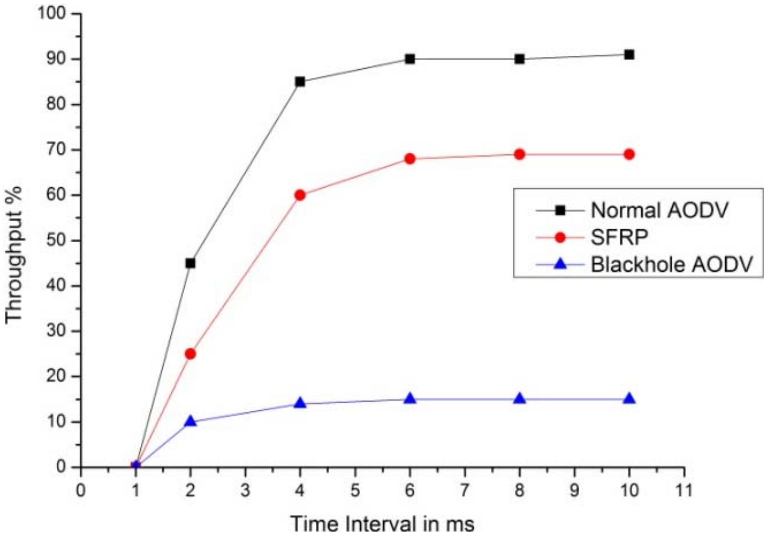
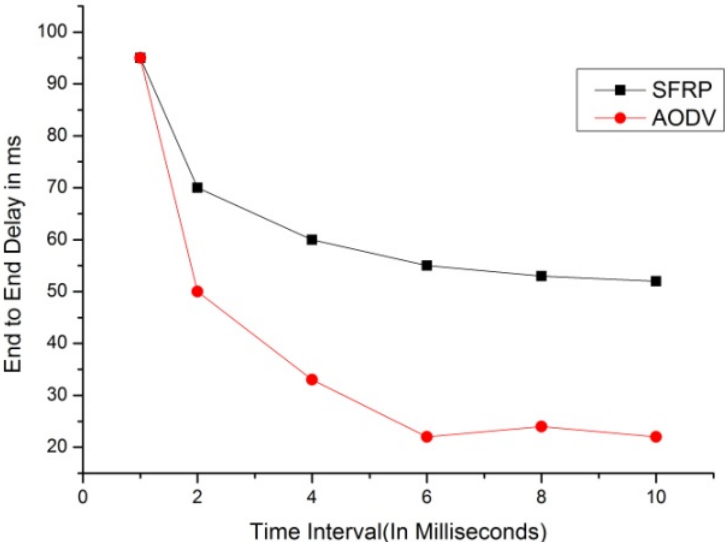


Figure 6 End to end delay calculation (see online version for colours)



As expected, black hole AODV has 70% packet loss while SFRP has around 25% as shown in Figure 5. Trusted AODV manages a modest 50%, which is better than black hole AODV. In the aspect of end to end delay, the new approach is giving the satisfactory results. While normal AODV has almost 100% throughput as shown in Figure 3, it is seen that trusted SFRP has 70% aggregate throughput which is better than the 20% of the AODV run in the presence of the Black hole without the trust. The loss of 30% in trust

AODV is due to time taken by the neighbouring nodes to judge the malicious behaviour of its neighbour.

SFRP has an end to end delay more than normal AODV as shown in Figure 6. This is the overhead associated with the relationship trust calculation algorithm.

7 Conclusions and future work

This paper gives a clear description of SFRP, and step by step explanation to achieve secure routing through family-based methodology. The proposed mechanism is specifically designed for MANETs. The purpose of this mechanism is to provide secure routing with minimum possible computation and to have minimum resource consumption. This task is accomplished by using trust instead of cryptography as cryptographic methods are known to be computationally intensive.

As future work, small constructive additions can be made in the proposed mechanism. In this approach if a node is malicious then that can never be revoked and it remains malicious throughout. Thus a mechanism can be developed which allows the malicious node to become a trusted node again based on its behaviour.

References

Al-Shurman, M., Yoo, S.M. and Park, S. (2004) 'Black hole attack in mobile ad hoc networks', *ACM Southeast Regional Conf.*

Bergamo, P., Maniezzo, D., Travasoni, A., Giovanardi, A., Mazzini, G. and Zorzi, M. (2004) 'Distributed power control for energy efficient routing in ad hoc networks', *Wireless Networks J.*, Vol. 10, No. 1, pp.29–42.

Deng, H., Li, W. and Agrawal, D,P. (2002) 'Routing security in wireless ad hoc networks', *IEEE Communication Magazine – Telecommunication Network Security*, University of Cincinnati, October.

Eichler, S. and Roman, C. (2006) 'Challenges of secure routing in MANETs: a simulative approach using DRI in wireless ad hoc networks', *IEEE International Conference on Mobile AdHoc and Sensor Systems*.

Hu, Y-C., Perrig, A. and Johnson, D. (2006) 'Wormhole attacks in wireless networks', *IEEE JSAC*, February, Vol. 24, No. 2, pp.19–42.

Hu, Y-C., Perrig, A. and Johnson, D.B. (2002) 'Ariadne: a secure on-demand routing protocol for ad hoc networks', *Proceeding of the 8th Annual International Conference on Mobile Computing and Networking*, ACM Press, pp.12–23.

Hu, Y-C., Perrig, A. and Johnson, D.B. (2003) 'Rushing attacks and defense in wireless ad hoc network routing protocols', *Proceedings of the 2003 ACM Workshop on Wireless Security (WiSe 2003)*, September, pp.30–40.

Huang, Y. and Lee, W. (2004) 'Attack analysis and detection for ad hoc routing protocols', *RAIS' 04: Proc. 7th Int'l. Symp. Recent Advances Intrusion Detection*, Sophia Antipolis, France, September.

Nandy, R. and Roy, D.B. (2011) 'Study of various attacks in MANET and elaborative discussion of rushing attack on DSR with clustering scheme', *International Journal Advanced Networking and Applications*, Vol. 03, No. 1, pp.1035–1043.

Pakzad, F. and Rafsanjani, M.K. (2011) 'Intrusion detection techniques for detecting misbehaving nodes', *Canadian Center of Science and Education*, January, Vol. 4, No. 1, pp.151–159.

Patwardhan, A., Parker, J., Joshi, A., Karygiannis, A. and Iorga, M. (2005) 'Secure routing and intrusion detection in ad hoc networks', *Third IEEE International Conference on Pervasive Computing and Communications*.

Razak, S.A., Furnell, S.M. and Brooke, P.J. (2004) 'Attacks against mobile ad hoc networks routing protocols', *5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting*, pp.147–152, Liverpool, UK.

Razzaque, M.A., Dobson, S. and Nixon, P. (2008) 'Cross layer self routing: a self-managed routing approach for MANETs', *Proceedings of the 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, IEEE Press, pp.284–290.

Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C. and Belding-Royer, E.M. (2002) 'A secure routing protocol for ad hoc networks', *Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP)*, November.

Wu, B., Chen, J., Wu, J. and Cardei, J. (2008) 'A survey on attacks and countermeasures in mobile ad hoc networks', in Xiao, Y., Shen, X. and Du, D-Z. (Eds.): *Wireless/Mobile Network Security*, Springer, UK.

Yan, Z., Zhang, P. and Virtanen, T. (2008) *Trust Evaluation Based Security Solution in Ad Hoc Networks*, Nokia Research Centre, Helsinki University, Finland.

Yi, S., Naldurg, P. and Kravets, R. (2001) *Security-Aware Ad-Hoc Routing for Wireless Networks*, Technical Report UIUCDCS-R-2001-2241, Department of Computer Science, University of Illinois at Urbana Champaign, August.