Asian Journal of Information Technology 15 (23): 4698-4704, 2016
ISSN: 1682-3915

Trust Based Routing Algorithm for Mobile Ad Hoc Networks

K. Mohaideen Pitchai
Department of Computer Science and Engineering,
National Engineering College, Kovilpatti, Tamil Nadu, India

Abstract: In this study a routing technique is proposed for Mobile Adhoc Networks (MANETs) and the nodes in the routing path are selected based on security. The trust value of the nodes are calculated using the number of neighborhood nodes, previous trust value of nodes, forwarded and generated packets sent by nodes and forwarding delay of nodes. The performance evaluation via simulation reveals that the proposed trust based routing achieves better performance than existing schemes in terms of identifying the malicious nodes and increasing the throughput of the network. Also the simulation is done over a range of environmental conditions such as number of malicious nodes and node mobility.

Key words: MANETs, malicious nodes, routing, trust, security

INTRODUCTION

Mobile Ad-hoc Networks (MANET) are a collection of mobile nodes which communicate with each other via multihop wireless links. Each node in MANETS acts as host and router at the same time. Due to openness of MANETS, nodes moving in any direction can join or leave the network at any time and can be publicly accessed without restriction. Mobile nodes are characterized with less memory, power and light weight features. The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links and spontaneous behaviour which demands minimum human intervention to configure the network. All nodes have identical features with similar responsibilities and capabilities. Hence, it forms a completely symmetric environment. Another important challenge is high user density and large level of user mobility and nodal connectivity is intermittent.

MANETs routing protocols are classified into two major categories, like Table-driven (Proactive) and on demand (Reactive). AODV (Ad hoc On Demand Distance Vector) offers low network utilization and uses destination sequence number to ensure loop freedom. The DSDV (Destination Sequence Distance Vector) protocol requires each mobile station to advertise to each of its current neighbours its own routing Table. At all instances, the DSDV protocol guarantees loop-free paths to each destination. DSR (Destination Sequence Distance Vector) computes the routes when necessary and then maintains them. DSR uses no periodic routing messages like AODV, thereby reduces network bandwidth overhead, conserves battery power and avoids large routing updates. MANETS is the suitable network for such type of application areas. All the existing MANETS protocols simply trust their neighbours and make a route through the neighbours. This kind of neighbour based routing is disturbed by intruders and internal attackers or malicious nodes. Threat to the nodes may be due to malicious nodes that generally harm the network with the manipulation of routing. Many routing protocols that have already been proposed are unable to identify such behaviour. There are several existing problems in Ad hoc network but there are fewer solutions. Generally, the existing systems provide either authentication level of security or a monitoring system (Nadkarni and Mishra, 2003). But these do not meet the challenges and security threats of MANETS. Various mathematical models have been used for calculating trust value. Based on the level of trust value the nodes will communicate with its one hop neighbours. In this proposed model, trust plays a major role in providing security which is being evaluated from Trust Based Routing (TBR) Algorithm. The idea of estimating trust rate among neighbours in a MANETS is probably a fast and effective way. But when the number of constraints increases, robust and accurate techniques are necessary, as it might affect the accuracy of the result. And hence a trust based computation model is proposed. The chapter discuss about the background details of the proposed system.

Back ground: In the ad hoc networks, routing protocol should be robust against topology update and any kinds of attacks. Unlike fixed networks, routing information in an ad hoc network could become a target for adversaries to bring down the network. The need for mobility in wireless networks necessitated the formation of the MANETS

working group for developing consistent IP routing protocols for both static and dynamic topologies. The different types of routing protocols explore several deterministic and random process models. Simply, a trust evaluation based method is needed along with these protocols.

AODV (Ad hoc On demand Distance Vector): It is a reactive protocol implying that it requests a route when needed. It does not maintain routes for those nodes that do not actively participate in a communication. An important feature of AODV is that it uses a destination sequence number which corresponds to a destination node that was requested by a routing sender node. The destination itself provides the number along with the route it has to take to reach from the sender node up to the destination. In this method security is a major constraint since the intruders can easily attack the nodes. Sometimes, malicious node can also involve in communication. Trust based secure routing AODV has been proposed but with a modified AODV with the trust value and leads to insecure and greater time complexity.

DSDV (Destination Sequence Distance Vector): It is a proactive routing protocol and is based on the distance vector algorithm. In proactive or Table-driven routing protocols, each node continuously maintains up-to-date routes to every other node in the network. Routing information is periodically transmitted throughout the network in order to maintain routing Table consistency. In case of failure of a route to the next node, the node immediately updates the sequence number and broadcasts the information to its neighbours. The Packet Delivery Ratio of this protocol compared to the other routing protocol is a low fraction value which shows the performance of the MANETs. When a node receives routing information then it checks in its routing table. In case, if the node finds that it has already entry into its routing Table then it compares the sequence number of the received information with the routing Table entry and updates the information. In DSDV, malicious node arbitrarily tampers the update messages to disrupt the routing algorithm. Thus, trust in the routing protocols is necessary in order to defend against hostile attacks.

DSR (Dynamic Source Routing): DSR is a reactive protocol. This protocol is one of the example of an on-demand routing protocol that is based on the concept of source routing. It is designed for use in multi hop ad hoc networks of mobile nodes. It allows the network to be completely self-organizing and self-configuring and does not need any existing network infrastructure. The DSR routing protocol discovers routes and maintains information regarding the routes from one node to other by using two main mechanisms: Route discovery-Finds the route between a source and destination and Route maintenance-In case of route failure, it invokes another route to the destination.

DSR has a unique advantage by virtue of source routing. This protocol takes much overhead like the maintenance of two different routing table information. The maximum speed of this routing protocol information varies inversely related with others. This protocol blindly trusts all other nodes not to be malicious and lead to several types of attacks. The major possible attacks include Replay attacks, wormhole attack and black hole attack due to the absence of trust

Literature review: Researches in Wang *et al.* (2009) present a Secure Destination-Sequenced Distance-Vector routing protocol (SDSDV) for ad hoc mobile wireless networks. The proposed protocol is based on the regular DSDV protocol. Within SDSDV each node maintains two one-way hash chains about each node in the network. Two additional fields which is AL (alteration) field and AC (accumulation) field are added to each entry of the update packets to carry the hash values. With proper use of the elements of the hash chains, the sequence number and the metric values on a route can be protected from being arbitrarily tampered. In comparison with the Secure Efficient Distance vector (SEAD) protocol previously proposed in the literature provides only lower bound protection on the metrics, SDSDV can provide complete protection. To evaluate the performance of SDSDV modified form of DSDV routing protocol that implemented in ns-2. Specifically, the increased the size of each routing update package to accommodate the authentication hash values in each Table entry required in SDSDV. This focuses on the evaluation of computation complexity between symmetric cryptograph and asymmetric cryptograph solutions in different scales of ad hoc networks.

The trust enhanced dynamic source routing protocol (Bhalaji *et al.*, 2009) is based on relationship among the nodes which makes them to cooperate in an Adhoc environment. The trust unit is used to calculate the trust values of each node in the network. The calculated trust values are being used by the relationship estimator to determine the relationship status of nodes. Trust enhanced DSR protocol increases the level of security routing and also encourages the nodes to cooperate in the adhoc structure. It identifies the malicious nodes and isolates them from the active data forwarding and routing. The routing misbehaviour is mitigated by including

components like watchdog and pathrater in the scheme proposed by Marti *et al.* (2000). Every node has a Watchdog process that monitors the direct neighbors by promiscuously listening to their transmission. No penalty for the malicious nodes is awarded.

The CONFIDANT protocol works as an extension to reactive source routing protocols like DSR (Buchegger and Le Boudec, 2002). The basic idea of the protocol is that nodes that does not forward packets as they are supposed to will be identified and expelled by the other nodes. Thereby, a disadvantage is combined with practicing malicious behavior.

The study Bayesian based confidence model for trust inference in MANET is based on service based scheme for computation of trust which takes into consideration the security requirement of a node as criteria for choosing the appropriate trust computation scheme. It can either choose to use direct trust, indirect trust or to form a trust network. It also proposes a modified Bayesian based confidence model (Elizabeth *et al.*, 2011) that gives an explicit probabilistic interpretation of trust for adhoc networks and describe trust inference algorithm that uses probabilistic sampling to infer the trust of a node based on the highest confidence estimation. It takes into account the security requirement for the application concerned and decides the scheme of trust computation.

Trusted AODV (Li *et al.*, 2004) is a secure routing protocol, this protocol extends the widely used AODV routing protocol and employs the idea of a trust model in subjective logic to protect routing behaviours in the network layer of MANET. TAODV assumes that the system is equipped with some monitor mechanisms or intrusion detection units either in the network layer or the application layer so that one node can observe the behaviours of its one-hop neighbours (Maurer, 1996). In the TAODV, trust among nodes is represented by opinion which is an item derived from subjective logic. The opinions are dynamic and updated frequently. Following TOADV specifications, if one node performs normal communications, its opinion from other nodes' points of view can be increased; otherwise, if one node performs some malicious behaviours, it will be ultimately denied by the whole network. A trust recommendation mechanism is also designed to exchange trust information among nodes. Dependable DSR without a trusted third party is a technique of discovering and maintaining dependable routes in MANET even in the presence of malicious nodes. Each node in the network monitors its surrounding neighbours and maintains a direct trust value for them. These values are propagated through the network along with the data traffic. This permits evaluation of the global trust knowledge by each network node without the need of a trusted third party. These trust values are then associated with the nodes present in the DSR link cache scheme. This permits nodes to retrieve dependable routes from the cache instead of standard shortest paths.

The distributed trust model makes use of a protocol that exchanges, revokes and refreshes recommendations about other entities. By using a recommendation protocol each entity maintains its own trust database. This ensures that the trust computed is neither absolute nor transitive. The model uses a decentralized approach to trust management and uses t rust categories and values for computing different levels of trust. The integral trust values vary from 1-4 signifying discrete levels of trust from complete distrust (-1) to complete trust (Marti *et al.*, 2000).

Each entity executes the recommendation protocol either as a recommender or a requestor and the trust levels are computed using the recommended trust value of the target and its recommenders. The model has provision for multiple recommendations for a single target and adopts an averaging mechanism to yield a single recommendation value. The model is most suitable for less formal, provisional and temporary trust relationships and does not specifically target MANET. Moreover, as it requires that recommendations about other entities be passed, the handling of false or malicious recommendations was ignored in their research.

In this study, a theoretical framework is proposed for trust modeling and evaluation. Here trust is a software entity. From this understanding of trust, an Algorithm is developed that address the basic rules for trust in a network.

MATERIALS AND METHODS

Proposed work

Trust based routing algorithm: The main contribution of this study is to provide a secure model based on trust computation. For this a TRUST BASED ROUTING ALGORITHM is proposed with the idea of managing the decentralized network effectively. It includes the Neighbour set table that contains the neighbour id of the source node. For each source their one hop neighbours will be listed. Neighbour set table also contains a self entity known as trust for each of the available neighbours. Based on the level of trust from the neighbour set Table the node is assigned as TH, TA, TL and NT (Table 1). The priority is given only for the TH and TA neighbour range. This study also provides the second level authentication of password checking for the neighbours in the higher priority level. After this the

Table 1: Trust entity

Entity	Full form	TBR value
TH	Trust high	0.76-1.00
TA	Trust average	0.51-0.75
TL	Trust low	0.26-0.50
NT	No trust	0-0.25

Source node will send RREQ Packet to the trusted node. Similarly, the routes are established on demand. The key framework of this paper is to check the level of trust with the neighbours available in the table. So, this provides a higher model of trust computation with simple mathematical equation.

Step 1: The source node will broadcasts HELLO packets to all its one hop neighbors in its transmission range. If an acknowledgement is received, then those nodes will be included in Neighbor Set Table (NST).

Step 2: In order determine the trust level of the neighbors', check whether the destination node is in source nodes NST. If it is true then calculate its trust value according to the Step 4.

Step 3: If the destination is not in the NST, then find the trust value of all of its neighbors in the NST.

Step 4: Compute the good level of trust TBR(y) among all the available neighbors. TBR(y) = sin(x) to calculate the trust value (y) based on a node's direct experience. Here the computation value is restricted between 0 and 1. The function for calculating the trust value is:

$$TBR(y) = \sin(c1 \times Prev_{trust} + c2 \times No_{neigh} + c3 \times Pac_{sent} + c4\ Delay_{Forward}) \quad (1)$$

where, c1-c4 are constants whose sum is equal to 1. Those values are determined during simulation. $Prev_{trust}$ is the previous trust value of node x. No_{neigh} represents the number of neighbor nodes of y. Pac_{sent} represents the packets forwarded and generated by x. $Delay_{Forward}$ represents the forwarding delay of node x.

Step 5: After calculating the trust value of all neighbors, they are categorized according to trust value ie. Trust High -TH (TBR value between 0.76 and 1), Trust Average TA (TBR value between 0.51 and 0.75), Trust Low-TL (TBR value between 0.26 and 0.5) and No Trust - NT (TBR value between 0 and 0.25).

Step 6: The neighboring nodes which fall under the category of NT will not be considered for routing. Rest of the three categories TH, TA and TL goes for the next level of security verification.

Step 7: The neighboring nodes with trust value TH will go for low level of encryption. Likewise nodes with trust values TA and TL will go for medium and higher level of encryption respectively. The encryption levels are classified based on the size of the key. 32, 64 and 128 bit keys for TH, TA and TL respectively.

Step 8: With these levels of security checks the source node establishes a route to its neighbor and the process proceeds still one hop neighbor is the destination.

Procedure for evaluating trust: The nodes in the neighbor Table are evaluated for trust based on the Eq. 1 mentioned in step 4 of the TBR algorithm. In this equation four important parameters are considered for calculating the TBR value. The $Prev_{trust}$ parameter specifies the previous trust value of the node. It represents the past activity of the node. The parameter Pac_{sent} is considered for determining the trust value in order to accommodate the severity of the traffic. Trust is an array that holds neighbor id for each trust entity. TMNODE is used to temporarily hold the neighbors:

Algorithim

```
For (each node I in neighbour table)
 {
if ( 0.76<TBR value<1.0)
{
assign_trust[i] = TH;
save TMNODE[j] = i;
j++;
}
else if (0.51 < TBR value<0.75)
{
assign_trust[i] = TA;
save TMNODE[k] = i;
k++;
}
 else if ( 0.26<TBR value< 0.5)
{
trust[i] = TL;
}
else
{
trust[i] = NT;
generate a warning message;
}
}
```

Flow chart: The flowchart in Fig. 1 explains the procedural steps of the proposed algorithm. The network is deployed first for a particular transmission range. Then the nodes within that range are identified by broadcasting Hello

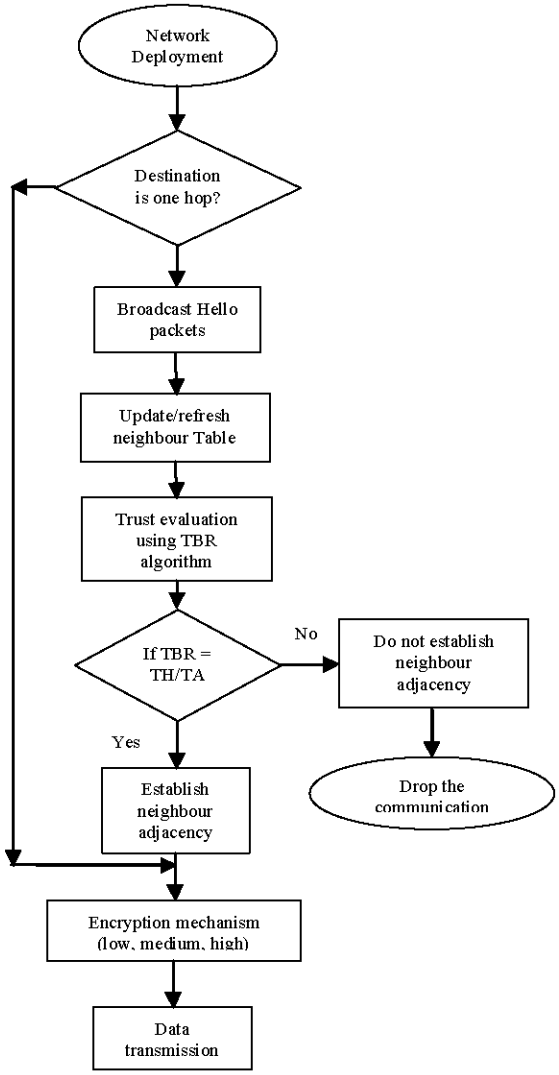

Fig. 1: The proposed alogorithim

packets. Applying the TBR algorithm for establishing neighbour adjacency and then evaluates the trust. And as a second level different levels of encryption technique are done with the trusted neighbours.

RESULTS AND DISCUSSION

Performance evaluation: Consider a MANET with all type of nodes which may be selfish or malicious as well as trusted node. Here in the illustrated example, (Fig. 2) there are eight nodes. The node 1 acts as source want to send data to destination node 8. When a node is ready for data transmission, first it should be aware of the neighbours. After getting information about its one hop neighbours,

Fig. 2: Trust evaluation using TBR

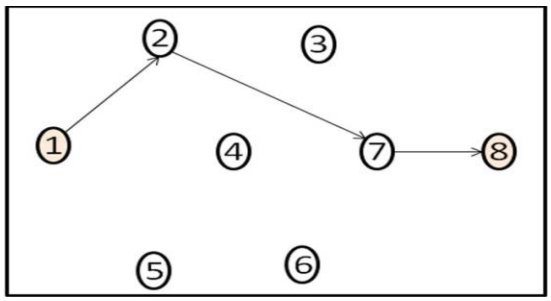

Fig. 3: Path establishment from source to destination

Table 2: Neighbour trust

Neighbour Id	Trust value
2	TH
4	NT
5	TL

the source now has to compare the level of trust among all of them from neighbour set table. For instance, (Fig. 3) node 1 has 2, 4 and 5 as its one hop neighbours. The neighbour set information is updated in the neighbour table. Applying TBR Algorithm, the source node will decide the trusted node and data packets are sent to that node. For node 2, the neighbor Table 2 contains 3, 7 and 6 as neighbors. Among these, node 7 has the highest trust. Now, node 7 will broadcasts Hello Packets to choose its neighbors. The node 7 has node 8 as its one hop which is the destination. This process continues until the exact path or the route to the destination is reached

To analyze the performance of the proposed protocol, it was simulated in a 1000×1000 m region. The transmission range was set to 25 m. The nodes were set to move at a speed to 10-20 m sec^{-1} with a pause time of 30 sec. CBR traffic was generated with the data payload size of 512 bytes. To calculate the value of TBR for each neighbor node the constants c1-c4 are assumed as 0.25. The parameters like time to first byte, throughput and percentage of attacks detected were measured.

The parameters Time Taken to receive First Byte (TTFB) after the connection has been setup was

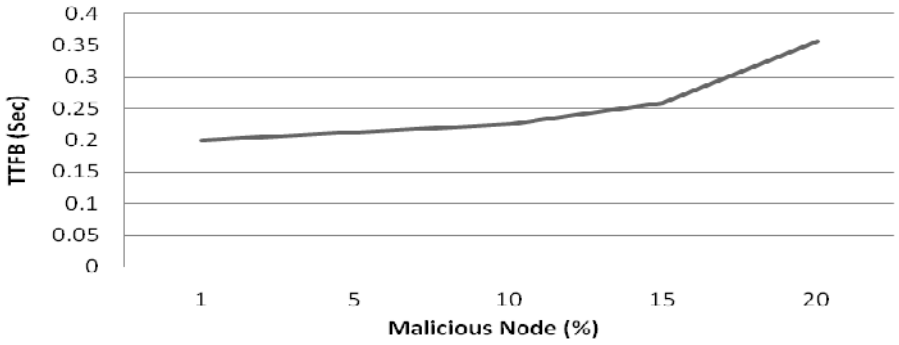

Fig. 4: Time to first byte vs. malicious nodes

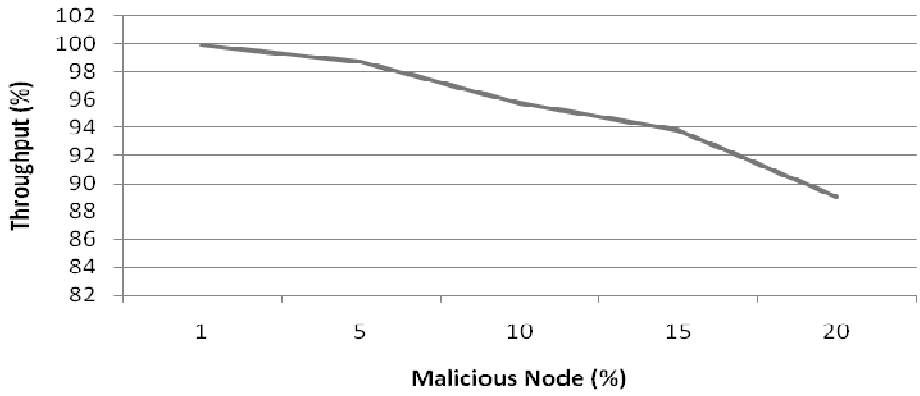

Fig. 5: Throughput vs. Malicious nodes

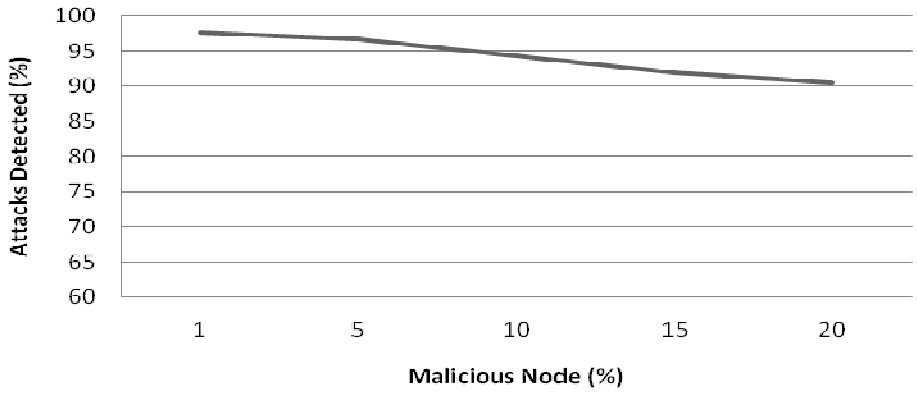

Fig. 6: Attacks detected vs. Malicious nodes

measured in each round of simulation and it seems to be consistent throughout the simulation as shown in Fig. 4. TBR algorithm is a reactive routing protocol which will collect routing information only on demand. The advantage of this algorithm is that it creates no extra traffic for communication along existing links and the connection setup delay is lower. The throughput of the nodes in the network seems to drop down with the increase in number of nodes in the network and this behavior is shown clearly in Fig. 5. Figure 6 shows a decreasing trend in the percentage of attacks detected in each rounds of simulation with increasing number of adversaries.

CONCLUSION

This study proposes a novel routing algorithm that relies on the trust of the neighbours to select a path in

routing the protocols to the destination. A TBR algorithm is proposed which calculates the trust worthiness of the neighbours in the network and prioritizes a path based on the calculated trust value.

REFERENCES

Bhalaji, N., A.R. Sivaramkrishnan, S. Banerjee, V. Sundar and A. Shanmugam, 2009. Trust enhanced dynamic source routing protocol for adhoc networks. World Acad. Sci. Eng. Technol., 49: 1074-1079.

Buchegger, S. and J.Y. Le Boudec, 2002. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 9-11, 2002, Lausanne, Switzerland, pp: 226-236.

Elizabeth, B.L., R. Aaishwarya, P. Kiruthika, M.N. Shrada and A.J. Prakash et al., 2011. Bayesian based confidence model for trust inference in MANETs. Proceedings of the International Conference on Recent Trends in Information Technology (ICRTIT), June 3-5, 2011, IEEE, Anna University, Chennai, ISBN:978-1-4577-0590-8, pp: 402-406.

Li, X., M.R. Lyu and J. Liu, 2004. A trust model based routing protocol for secure ad hoc networks. Proceedings of the IEEE Conference on Aerospace, Volume 2, March 6-13, 2004, Big Sky, Montana, USA., pp: 1286-1295.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehaviour in mobile Ad Hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, August 6-11, 2000, Boston, MA., USA., pp: 255-265.

Maurer, U., 1996. Modelling a Public-Key Infrastructure. In: European Symposium on Research in Computer Security, Bertino, E., H. Kurth, G. Martella and E. Montolivo (Eds.). Springer, Berlin, Germany, pp: 325-350.

Nadkarni, K. and A. Mishra, 2003. Intrusion detection in MANETs-the second wall of defense. Proceedings of the 29th Annual Conference of the IEEE Industrial Electronics Society, Volume 2, November 2-6, 2003, IEEE Computer Security, USA., pp: 1235-1238.

Wang, J.W., H.C. Chen and Y.P. Lin, 2009. A secure DSDV routing protocol for ad hoc mobile networks. Proceedings of the 5th International Joint Conference on INC, IMS and IDC, NCM'09, August 25-17, 2009, IEEE, Taichung, Taiwan, ISBN:978-1-4244-5209-5, pp: 2079-2084.