Neural, Parallel, and Scientific Computations 23 (2015) 487-498

DYNAMIC-TRUST MODEL FOR MONITORING MALICIOUS NODE OSCILLATING BEHAVIOR IN MANET USING SATISFACTION AND FEEDBACK CREDIBILITY

PARKAVI. K [1], SWAMINATHAN. A [2], VIVEKANANDAN. P [3]
[1, 2] Computer Science and Engineering, Anna University, Chennai, India.
[3] Computer Centre, Anna University, Chennai, India.

Abstract: Routing in an mobile ad-hoc network (MANET) is an active research area in recent years. It still faces challenges such as limited physical security, node mobility, and limited resources such as bandwidth and storage. Trust plays a growing role if security in an open environment where unknown devices can join or leave the system at any time. In this paper, a suite of efficient secure routing protocol referred as Dynamic-trust model is developed, which will be based on the trust level of individual nodes within the ad-hoc network. The design of routing protocols for mobile ad-hoc networks rarely contemplates in most hostile environments. Consequently, it is common to add security extensions afterwards. One feasible way to minimize the threats is to evaluate the trust and reputation of the interacting neighbors. Many trust models have done so, but they fail to properly evaluate trust when malicious agents start to behave in an unpredictable way. Moreover, these models are ineffective in providing quick response to a malicious node's oscillating behavior. In this dynamic-trust model, security is inherently built into the routing protocol where each node evaluates the trust level of its neighbors based on a set of attributes. A secure route is established based on a confidence level prescribed by a user in terms of these attributes. Analytical and simulation results are presented to evaluate the performance of the proposed scheme.

Keywords*:* Routing, Dynamic-trust, malicious, MANET

1. INTRODUCTION

Mobile ad-hoc network (MANET) is a wireless self-configuring network consisting of infinite number of mobile devices temporarily and they are interconnected into a network by any number of wireless connections. They dynamically self-organized in arbitrary and temporary network topologies. The network elements may leave or join anywhere at any time in an ad-hoc networks. Each MANET device may independently move in any direction and thus, often change its connections to other devices within the network. Each of the nodes may forward traffic not necessary for its needs; hence every node within the network may be a router. That is why they are not dependent on network infrastructure since their structure is created by own networking capacities of network elements. Thus, the bandwidth and energy available to nodes are limited and represents the most important inherent resources, so the academic community makes enormous efforts in research and development of different types of protocols to answer the demands for both efficiency and security.

1.1 SECURITY REQUIREMENTS

The security requirements (Dragan Mladenovic & Danko Jovanovic, 2012) of the MANET's are

Received August 1, 2015

- Confidentiality represents the capability to prevent access to information by unauthorized users or nodes. Since MANETs use open medium, all users of this medium have the access to information within certain transmission range. The basic way to preserve confidentiality is encryption and alternative is to limit the emission of data through the use of directional antennas.

Authentication is the ability of an unambiguous confirmation of node identity and simultaneously the ability to prevent taking false identity. However, in infrastructure wireless networks ,it is possible to establish a central authority (functioning as a router, base station or access point), which is not the case for MANETs. So this requirement must be fulfilled through other methods primarily through routing protocols and inbuilt access control mechanisms.

- Integrity represents the ability to prevent an unauthorized change or destruction of messages being transmitted within MANET, as well as prevent subsequent messages from the attacker after the unauthorized change. Interception and change of data in a wireless medium is very frequent.
- Non-repudiation is the inability of any node within a MANET to negate the fact that it is a sender of a message. This requirement is provided by producing a signature for every message. In an usual encryption procedure by the public key method, every node in a MANET signs a message by application of a private key. All other nodes verify the signed message with this node's public key, therefore the node cannot negate its signature that is attached to the message.
- Availability represents the availability of all network services and resources to legitimate network users, which is essential for preserving the network structure during the attacks. Access control is a procedure for prevention of unauthorized access and use of network systems and resources. Different mechanisms are used in order to provide these security requirements. The first line of defense is conventional mechanisms such as authentication, access control, encryption and digital signature. The second line of defense is intrusion detection systems and different cooperation enforcement mechanisms enabling the defense from attacks, improving the cooperation within the network and eliminating selfish behavior of nodes.

1.2 ROUTING

The goal of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node (Shen et al., 2006). Routing protocols in a MANET can be classified into two categories that are reactive routing protocols (e.g., AODV) and proactive routing protocols (e.g., OLSR). In reactive routing protocols, nodes find routes only when they must send data to the destination node whose route is unknown. On the other hand, in proactive protocols, nodes periodically exchange topology information and hence the nodes can obtain route information any time they must send data.

a) Route Discovery: A mechanism initiated by a node upon the arrival of a new traffic session in order to discover a new path to a node *j*. Node *i* floods the whole network with route request (RREQ) packets. Upon receiving the RREQ packet, node *j* sends out a route reply packet (RREP) along the reverse path to *i*. As a result, node *i* usually gets a shortest path to node *j*.

b) Route Maintenance: a mechanism by which a node is notified that a link along an active path has broken, such that it can no longer reach the destination node *j*

through that route. Upon reception of a notification of route failure, node i can initiate a route discovery again to find a new route for the remaining packets destined to j.

In reactive routing protocols, each node does not maintain routing tables before a routing task is triggered. They only find a route on demand by flooding the network with RREQs i.e., before sending data packets the sender broadcasts router request and initiates a route discovery process. If a link breakage is detected during packet delivery, a new RREQ is generated. The main disadvantages of such algorithms are high latency time in finding routes and excessive flooding when traffic load is high.

Assume that a successful delivery between source node S and destination node U takes K hops, that at the first step a route discovery is initiated at S and that after time $\Delta 0$ source node S receives a RREP and starts sending data packets. Assume that a link breakage occurs at a relay node F with probability pi and then a new RREQ is generated for F and that it takes time Δi to restart delivery. Let us suppose that the transmission delay for any link i is Ti. Then the end-to end delivery delay Dp between S and U can be formulated as

$$D_p = \Delta_0 + \sum_{i=1}^{k} (p_i \Delta_i + T_i)$$

Compared to the local recovery time in proactive routing protocols, the route discovery time in reactive routing protocols is much larger.

1.3 NODE CLASSIFICATION

In a wireless ad-hoc network, node cooperation in a routing process is an essential requirement to maintain protocol operations and network connectivity (Tseng et al., 2006). However, since every node is an autonomous system, it may decide how to act in the network by itself. Considering the potential impacts of various misbehaviors, additional assumption introduced that all nodes operate independently in the following four states:

- **Cooperative state**: In this state, a node complies with all routing and forwarding rules, i.e., being able to initiate and respond to route discoveries correctly and forward control and data packets for others at the best effort.
- **Selfish state:** In this state, a node can initiate and respond to route discoveries for its own purpose but may not forward control or data packets for others for the sake of power saving.
- **Malicious state:** In this state, a node launches DoS attacks on the network layer, e.g., being cooperative in the routing stage but reluctant in forwarding data packets or disrupting legitimate path selections by broadcasting fake route replies**.**
- **Failed state:** In this state, a node is unable to initiate or respond to route discoveries.

1.4 NODE BEHAVIOR TRANSITIONS

Mobile ad-hoc networks are complex and dynamic systems due to unexpected random node behaviors. In real networks, the behavior of a node may change at any time due to various reasons. For example, a node can be failed due to energy depletion or even a turn-off of transceivers triggered by end users, or a node's security can be compromised by other attackers so that the node is utilized to launch new attacks. In this work, it is assumed that a node may change its behavior as follows:

i)A cooperative node is exposed to become failed due to various reasons such as energy exhaustion, misconfiguration, and so on. It is also prone to be configured on purpose as a selfish one for the sake of power saving or to be compromised as a malicious node.
ii) It is possible to convert a selfish node to be cooperative again by means of proper configurations. A selfish node can become malicious due to being compromised or failed due to power depletion. A malicious node can become a failed node, but it will no longer be considered to be cooperative or selfish even if its disruptive behaviors are intermittent only.
iii) A failed node can become cooperative again if it is recovered and responds to routing operations. The above assumptions do not specify any particular reason for a behavior transition, so they can provide a general exposure to the most common behavior transitions and are applicable to a wide range of network scenarios.

2. RELATED WORK

The major task of the routing protocol is to discover the topology to ensure that each node can acquire a recent map of the network to construct routes to its destinations. Several efficient routing protocols have been proposed for MANET. These protocols generally fall into one of the two major categories mentioned. In reactive routing protocols, such as Ad-hoc On Demand Distance Vector (AODV) protocol (Perkins et al., 2003), nodes find routes only when they must send data to the destination node whose route is unknown. In contrast, in proactive routing protocols, such as OLSR (Clausn & Jacquet, 2003) nodes obtain routes by periodic exchange of topology information with other nodes and maintain route information all the time.

2.1. ATTACKS

Based on the behavior of attackers, attacks against MANET can be classified into passive or active attacks. Attacks can be further categorized as either outsider or insider attacks. With respect to the target, attacks could be also divided into data packet or routing packet attacks. In routing packet attacks, attackers could not only prevent existing paths from being used, but also spoof non-existing paths to lure data packets to them. Several studies (Hu & Perrig, 2004; Kannhavong et al., 2006; Kannhavong et al., 2007) have been carried out on modeling MANET routing attacks. Typical routing attacks include black-hole, fabrication, and modification of various fields in routing packets (route request message, route reply message, route error message, etc.). Some research efforts have been made to seek preventive solutions (Hu et al., 2003; Hu et al., 2005) for protecting the routing protocols in MANET. Although these approaches can prevent unauthorized nodes from joining the network, they introduce a significant overhead for key exchange and verification with the limited intrusion elimination. Besides, prevention-based techniques are less helpful for defending from malicious insiders who possess the credentials to communicate in the network.

Numerous intrusion detection systems (IDS) for MANET have been recently introduced. Due to the nature of MANET, most IDS are structured to be distributed and have a cooperative architecture. Similar to signature-based and anomaly-based IDS models for wired network, IDS for MANET use specification-based approaches and statistics-based approaches. Specification-based approaches, for example

DEMEM (Tseng et al., 2006) monitor network activities and compare them with known attack features, which are impractical to cope with new attacks. On the other hand, statistics-based approaches, such as Watchdog (Kannhavong et al., 2007) and Lipad (Anjum & Talpede, 2004) compare network activities with normal behavior patterns, which result in higher false positives rate than specification-based ones. Because of the existence of false positives in both MANET IDS models, intrusion alerts from these systems always accompany with alert confidence, which indicates the possibility of attack occurrence. Intrusion response systems (IRS) for MANET are inspired by MANET IDS. T.View (2006), Liu et.al (2004) isolate malicious nodes based on their reputations. Their work fails to take advantage of IDS alerts and simple isolation of nodes may cause unexpected network partition. Wang et al. (2007) bring the concept of cost-sensitive into MANET intrusion response which considers topology dependency and attack damage. The advantage of our solution is that we integrate evidences from IDS, local routing table with expert knowledge to estimate risk of attacks, and countermeasures with a mathematical reasoning approach.

2.2 TRUST

Bayesian network-based trust model (Anupam Das & Islam, 2012) believes that trust is multidimensional and nodes need to evaluate trust from different aspects of an node's capability. This model uses Bayesian network and Bayesian probability to calculate trust. This model's main flaw lies in the authors' assumption that all the nodes have identical Bayesian network architecture which is unrealistic because different nodes have different requirements which lead to different network architecture. In the case of aggregating recommendation from other nodes, this model assumes that all the nodes are truthful in providing their feedbacks. This assumption is also not realistic as malicious nodes will often provide false feedback to other nodes to disrupt the system.

Eigen Trust (Wang & Vassileva, 2003) aggregates the local trust values of all nodes to calculate the unique global trust value of a given node. A node depends on some pretrusted nodes for trust evaluation in absence of trustworthy recommenders. Even though Eigen Trust may work well in social network infrastructure where pretrusted neighbors (nodes) are likely to be trustworthy, but in the case of other multiagent systems like P2P, Eigen Trust poses a few problems. First, in P2P network, such predetermined trustworthy nodes are not readily available. Second, depending on these pretrusted nodes creates vulnerability in the sense that if some of these pre-trusted nodes get compromised, then it will be much easier to launch a large-scale malicious attack. The trust model proposed by Wen et al. (2004) is similar to EigenTrust, but it does not consider the use of pretrusted nodes in the calculation of trust. Dou's model reduces iteration cost and punishes malicious behavior, but does not consider the punishment of dishonest recommenders.

.

PeerTrust (Tseng et al., 2006) computes the trustworthiness of an node as normalized feedback weighted against the credibility of feedback originators. In PeerTrust,five factors are defined for computing the trustworthiness of nodes among which three factors are basic trust parameters while the remaining two are adaptive factors. PeerTrust uses personalized similarity measure to compute the credibility of recommenders and it uses this credibility measure to weight each feedback submitted by the recommenders. PeerTrust's main drawback is that it has to retrieve all the transactions within the recent time window (which may contain a large number of

transactions) to compute the trust of an node. So, the trust evaluation process is both computationally and spatially expensive. Furthermore, all the transactions in the retrieved window is given equal significance but recent transactions should be given higher weight than past transactions.

FCTrust (Ebinger & Bismeyer, 2009) uses transaction density and similarity measure to define the credibility of any recommender providing feedback as opposed to (TView, 2006) which uses global trust to weigh the quality of feedbacks. In other words, FCTrust differentiates the role of providing feedbacks from that of providing services. However, FCTrust's main drawback is that in computing direct trust (DT), it retrieves all the transactions performed within a time frame. This imposes storage overhead. Moreover, the simple averaging function used to define local trust assigns equal weight to all the transactions but realistically, recent transactions should be given more importance than historical transactions. Another drawback of FCTrust is that it assigns equal degree of reward and punishment in computing similarity but the degree of punishment should be greater than that of reward. SFTrust computes service trust as a weighted average of local trust and recommendation trust, but the weight itself is static and as a result, it cannot properly accommodate the experience gained by the evaluating node over time.

Trust-based intrusion detection has received much attention in the literature because of its elasticity against uncertainty and resiliency against attacks. Wang et al. (2007) proposed an intrusion detection mechanism based on trust for mobile ad-hoc networks (MANETs). They employed the concepts of evidence chain and trust fluctuation to evaluate a node in the network. The evidence chain detecting misbehaviors of a node and the trust fluctuation reflecting the high variability of a node's trust value over a time window. Ebinger et al. (2009) introduced a cooperative intrusion detection method also for MANETs based on trust evaluation and reputation exchange. They split the reputation information into trust and confidence for reputation exchanges and then combine them into trustworthiness for intrusion detection. Liu et al. (2004) modeled trust evaluation as a path problem and used path and distance to combine opinions such that two nodes can establish an indirect trust relation without previous direct interactions.

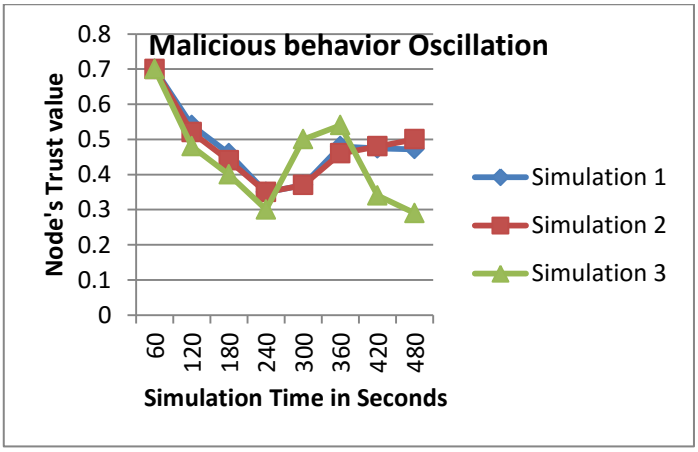

Figure 1.Trust value oscillation

With the increment of the simulation time, few nodes are detected as malicious node by the network As is shown in Figure 1, in order to cheat a high trust value, a malicious node makes good performance in a time interval (240 s –360 s), and then

behave badly in the third simulation. It is observed that the proposed Dynamic-trust model can effectively reduce the hazards from such node. The existing trust models are not successful in preventing from this oscillating behavior of malicious nodes and the node's trust value based on those models varies a lot.

3. DYNAMIC-TRUST MODEL

The main objective of this paper is to provide a Dynamic-trust computation model for effectively monitor the security of network even in the presence of highly oscillating malicious behavior. This model also provides a data forwarding scheme for proper distribution of packets among the various nodes in the routing path. A number of parameters have been considered in this Dynamic-trust model for computing the trust of a node. Now, some of these parameters have been previously discussed but none of these models can fully cope with the strategic adaptations made by malicious nodes. The mathematical and logical definitions used for these parameters also cannot reflect the true scenarios faced in real life. Moreover, none of these mentioned models have considered the wide range of parameters that are mentioned in this scenario. In the following sections, the mathematical expressions used for calculating some of the parameters are redefined to present the new Dynamic-trust model. It is assumed that node *p* (called evaluator) needs to calculate the trustworthiness of node *q* (called the neighbor node) for the trust evaluation.

3.1 SATISFACTION

Satisfaction function measures the degree of satisfaction for a node which has about a forwarding node. In other words, it keeps record of the satisfaction level of all the transactions that a node makes with another node. However, instead of storing all of the transaction history, an exponential averaging update function is defined to store the value of satisfaction. This greatly reduces the storage overhead and at the same time assigns time relative weight to the transactions. Let $satis_n^t(p,q)$ represent the amount of satisfaction node *p* has upon node *q* based on its data forwarding up to *n* transactions in the t^{th} time interval. The satisfaction update function is defined as follows:

$$satis_n^t(p,q) = \beta * satis_{curr}(p,q) + (1-\beta) satis_{n-1}^t(p,q)$$

Threshold value β is set to 0.25.

3.2 FEEDBACK CREDIBILITY

Feedback credibility is used to measure the degree of accuracy of the feedback information that the recommending node provides to the evaluator. Normally, it is assumed that good nodes always provide true feedback and malicious nodes provide false feedback. However, this is not always the real scenario as good nodes might provide false feedbacks to their competitors and malicious nodes might occasionally provide true feedbacks to hide their real nature. So, feedback credibility is needed to determine the reliability of the feedback. During trust evaluation, feedbacks provided by nodes with higher credibility are trustworthy, and are therefore weighted more than those from nodes with lower credibility.

Let $Feed_n^t(p,q)$ represent the feedback credibility of node q from node p's perspective.

$$Feed_n^t(p,q) = 1 - \ln(satis(p,q)) / \ln \omega$$

where $\omega = 0.01$ represents the lowest allowed value of satisfaction. By derivation, feedback credibility is a direct logarithmic function of satisfaction for its slow rise to the highest attainable value. This implies that the nodes with higher satisfaction with respect to the evaluating agent have higher feedback credibility.

3.3 DIRECT TRUST

Direct trust also known as local trust represents the portion of trust that a node computes from its own experience about the neighbor node. Let $DTrust_n^t(p,q)$ represent the direct trust that node p has upon node q up to n transactions in the t^{th} time interval. The satisfaction measure is used to define direct trust as follows:

$$DTrust_n^t(p,q) = satis_n^t(p,q)$$

Since satisfaction is computed by the node's own experience. So, if node q provides good service, then node p will rate it with a high satisfaction value and as a result, node q will obtain a high local trust rating from node p's perspective.

3.4 DYNAMIC-TRUST METRIC

This is the actual trust value used in prioritizing all nodes. It is computed from node's satisfaction value and feedback credibility.

$$Dynamic-Trust_n^t(p,q) = Feed_n^t(p,q) * satis_n^t(p,q) + DTrust_n^t(p,q)$$

For a node, to attain a high overall trust value it must behave cooperatively and at the same time must not
lower trust satisfaction. Therefore, a node will use *Dynamic-Trust* value to select the neighbor with the highest trust value.

3.5 DATA FORWARDING THROUGH TRUSTED NODES

In this section, an algorithm for data forwarding through the trusted nodes is proposed.

Algorithm 1. Selection of load balanced node

Input set:Source node p,Set of intermediate nodes S, Destination q
Output: Random neighbor with good trust value and less load

```
for each x ∈ s
    Compute Trust (p,x)
      if Trust (p, x) > β then        /* β -Threshold value of trust  */
        G ← G ∪ {x}                   /* G-Good trust nodes  */
      end if
 end for
```

```
if G ≠ 0 then
    for each x ∈ G do
        Compute load N (p, x)              /*Number of previous transmissions */
    end for
    Sort G in increasing order of load N
    return neighbor node x with the smallest load N
else
Total trust ← 0
for each x ∈ U do                          /* Unknown trust neighbors  */
     Total trust ← Total trust +Trust (p, x)
end for

if Total trust > 0 then
   for each x ∈ G do
   Compute Probability (p, x)
   end for
return any neighbor node x randomly
end if
else
return node q
```

For selective scenario, the trusts of nodes who respond to a transaction request are first computed and then a node with the highest trust value is selected. However, in this scenario, the node with the highest trust value will have immense workload while other capable nodes with slightly lower reputation will have considerably less workload. The problem that will arise from this disproportionate allocation of workload is that the quality of service and battery power will fall greatly due to the heavy workload present at the highly trusted nodes. So, a load-balancing algorithm is required to fetch for sustaining good security level.

4. PERFORMANCE EVALUATION

In the simulations, a version of Network Simulator (NS-2) is used and it includes wireless extensions developed by the CMU Monarch project group. To compare the performance of Dynamic-trust with other existing trust models, an evaluation index named, successful transaction rate (STR) is used. STR is described as the ratio of the number of successful transactions to the total number of transactions. Since computed trust values may range differently for different trust models, other form of evaluation index such as trust computation error is not suitable for comparison. It really does not matter what range of trust value is assigned to a node, what matter is how efficiently the model can filter out malicious nodes based on the calculated trust value. In other words, the relative ranking of nodes based on their trust values is comparable and that's why STR value only computed for comparison with other models.

In the second experiment, it is observed that the impact of collusion caused by malicious nodes on STR. Due to the ease of accessibility, networks today are home to a significantly large number of malicious nodes, especially the military environments holds great threats as it terms with malicious nodes .In other words, threats and risks are implicitly increasing as network applications are widening. So, in such networks, Dynamic-trust would be the best option.

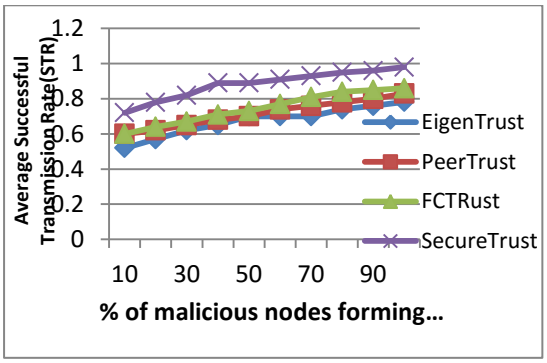

Fig.2 .Comparing Dynamic-trust with other models in terms of average STR against malicious behavior

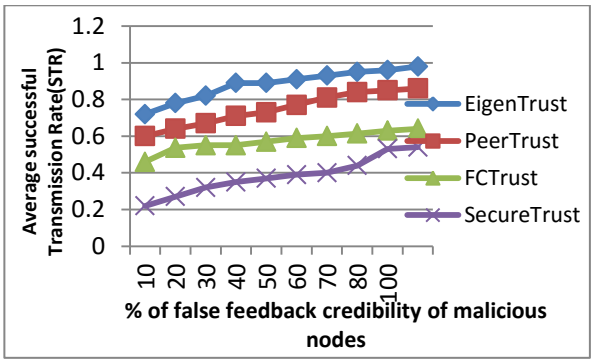

Fig.3 .Comparing Dynamic-trust with other models in terms of average STR against false feedback

In the second experiment, it is observed that the impact of false feedback by malicious nodes. So, for this simulation is done with malicious count to 90 percent because as the number of malicious nodes increase, their collusive impact becomes greater. Figure 2 represents the computed STR against collusion. Due to the experimental randomness, the gradient of the curves may vary from experiment to experiment. In Figure 3, it is shown that, Dynamic-trust shows superiority over others. The main reason behind this is the feedback credibility measure which filters out false feedbacks. In order to attain a high credibility, malicious nodes would have to provide honest feedback which goes against their true nature.

5. CONCLUSION

Like any other reputation model, this Dynamic-trust model assists nodes to choose reputed nodes while avoiding untrustworthy ones. However, reputation-based trust mechanism also introduces vulnerabilities such as shilling attacks where adversaries attack the system by submitting false ratings to confuse the system. Shilling attack is often followed by collusion attack where malicious nodes collaborate to raise each other's rating by making fake transactions. Dynamic-trust prevents such threats by assigning feedback credibility to each feedback provider. The Dynamic-trust discards feedbacks submitted by malicious nodes and thereby avoids collusion attack. Another challenging threat that most trust models fail to handle is the dynamic personality of malicious nodes. Dynamic-trust keeps track of sudden rise and fall of trust and thereby can easily penalize such oscillating behavior. A novel trust computation model is presented called Dynamic-trust for evaluating nodes in insecure environments. Dynamic-trust can ensure secured communication among nodes by effectively detecting strategic behaviors of malicious nodes. In this paper, a comprehensive mathematical definition of the different factors related to computing trust is given. Simulation results indicate, compared to other existing trust models, Dynamic-Trust is more robust and effective against attacks from opportunistic malicious nodes.

REFERENCES

[1] Dragan Mladenovic,Danko Jovanovic.Mobile Ad Hoc Networks Security,International Scientific Conference,Serbia,(2012)1-7.
[2] X. Shen, and D.Z. Du , Y. Xiao, *Wireless/Mobile Network Security*, Spinger,2006.

[3] Ricardo Puttini, Jean-Marc Percher, Ludovic MC, Rafael de Sousa.A fully distributed IDS for MANETs,IEEE (2004) 331-338.
[4] Ziming Zhao,Hongxin Hu,Gail-Joon Ahn,Ruoyu Wu. Risk-Aware Response for Mitigating MANET Routing Attacks,IEEE *GLOBECOM* (2010).
[5] C. Perkins, E. Belding-Royer, and S. Das. RFC3561: Ad hoc on-demand distance vector (AODV) routing, 2003.
[6] T. Clausen and P. Jacquet. RFC3626: Optimized Link State Routing Protocol (OLSR). RFC Editor United States, 2003.
[7] Y. Hu and A. Perrig. A survey of secure wireless ad hoc routing. IEEE Security and Privacy magazine, 2(2004) 28–39.
[8] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto.A study of a routing attack in OLSR-based mobile ad hoc networks.International Journal of Communication Systems, 20(2007) 1245–1261.
[9] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour. A collusion attack against OLSR-based mobile ad hoc networks,*GLOBECOM*, 2006.
[10] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour. A Survey of routing attacks in mobile ad hoc networks. *IEEE Wireless Communications*, 2007.
[11] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. Wireless Networks, 11(2005) 21–38, 2005.
[12] Y. Hu, D. Johnson, and A. Perrig. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks, Ad Hoc Networks,1(2003) 175–192.
[13] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. Wireless Networks, 11(2005) 21–38.
[14] Y. Hu, D. Johnson, and A. Perrig. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks,Ad Hoc Networks,1(2003) 175–192.
[15] C. Tseng, S. Wang, C. Ko, and K. Levitt. Demem: Distributed evidencedriven message exchange intrusion detection model for manet. Recent Advances in Intrusion Detection, Springer, (2006) 249–271.
[16] C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt. A Specification-Based Intrusion Detection Model for OLSR,Lecture Notes In Computer Science, 2006.
[17] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks,Proceedings of the 6th annual international conference on Mobile computing and networking, ACM (2000) 255–265.
[18] F. Anjum and R. Talpade. Lipad: lightweight packet drop detection for ad hoc networks,IEEE 60th Vehicular Technology Conference (2004),1233–1237.
[19] T. View. Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Areas in Communications, 24(2006) 305–317.
[20] J. Liu and V. Issarny. Enhanced Reputation Mechanism for Mobile Ad Hoc Networks. Lecture Notes In Computer Science,(2004)48–62.
[21] S. Wang, C. Tseng, K. Levitt, and M. Bishop. Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks, Lecture Notes In Computer Science, 2007.
[22] Anupam Das ,Mohammad Mahfuzul Islam. SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems, IEEE Transactions On Dependable And Secure Computing, 9(2012),261-275.
[23] Y. Wang and J. Vassileva. Bayesian Network-Based Trust Model, Proc. IEEE/WIC Int'l Conf. Web Intelligence (2003) 372-378.

[24] P. Ebinger and N. Bissmeyer.TEREC: trust evaluation and reputation exchange for cooperative intrusion detection in MANETs, Proc.Communications and Networking Services Research Conference,(2009) 378–385.