Asian Journal of Information Technology 16 (2-5): 181-189, 2017
ISSN: 1682-3915

Detection of Malicious Nodes using Enhanced Integrated Dynamic Trust Recommender in MANET

[1]Ramesh Ponnusamy, [2]H. Abdul Raufh and [1]S. Malarvizhi
[1]Department of Computer Technology, Anna University, Chennai, India
[2]Dhaanish Ahmed institute of Technology, Coimbatore, India

Abstract: Trust and reputation models are utilized in the security mechanisms of MANET to deal with selfish and misbehaving nodes and ensure safe delivery of packets from source to destination. The calculation of trust values and its propagation between the nodes form the rubric of these trust models. But its effectiveness is often degraded by the propagation of fake trust values via. dishonest recommendations particularly in environments like MANET due to the lack of centralized administration and mobility of nodes. However, dealing with dishonest recommendation attacks is a highly challenging task. We propose an enhanced integrated dynamic trust recommender that filters out dishonest recommendations by clustering, filtering and selecting the recommended trust values based on certain criteria. This makes the trust reputation model more robust and accurate in the dynamically changing MANET environment.

Key words: Trust and reputation model, Mobile Ad Hoc Network, recommendation management, trust reputation, enhanced integrated dynamic, MANET

INTRODUCTION

A mobile ad hoc network is an autonomous collection of continuously self configuring mobile devices/nodes connected without wires. These nodes act as a host and router and work together to ensure the continuous availability of network services. It is therefore essential that these nodes operate in a trustworthy manner and cooperate with one another for successful transmission of packets. Lack of infrastructure and central authority in MANET makes it vulnerable to attacks launched by misbehaving nodes displaying selfish and malicious behaviours (Shabut *et al*., 2015). In order to cope with the uncertainties caused by such malicious nodes, trust level of a node is analyzed before conducting transactions with it (Shakshuki *et al*., 2013). Thus trust is used in the security mechanisms of MANET to prevent an untrustworthy node from affecting the quality and reliability of data in the network. Trust in MANETs is the level of belief that one node can place on another to perform a specific action based on the past observation of behavior of that node (Jichkar and Chandak, 2014).

Although, trust can be categorized in many ways, the two broad categories are based on the method of evaluation. The trust value calculated based on the direct observations collected by node itself is known as direct trust whereas the trust calculated based on the recommendations propagated by other nodes in the network is known as indirect trust (Jichkar and Chandak, 2014). It is not possible to calculate the trust of a node in the absence of prior interactions or observations. In such cases recommendations from other nodes that have previously interacted or observed the node can be used for trust computation. This helps in identifying and avoiding malicious nodes prior to interaction (Biswas *et al*., 2014). Recommendations also contribute to selection of secure routing path, eliminating the need for direct interactions from the past. However, a false recommendation from other nodes about legitimate nodes has to be dealt with carefully as it curtails the effectiveness of the trust model. Similarly recommending high trust values for a malicious node can wreck considerable damage, thereby affecting the reliability and quality of data.

In this study, we have considered various regulations to come with an integrated measure to address the problem of dishonest recommendations. The recommendation based trust model ensures time and location consistent honest recommendations by considering the number of interactions with the evaluated node, similarity of view with the evaluating node and service reputation.

Literature review: In the trust model proposed by Marchang and Datta (2012) every node maintains a trust value for each of its neighbors (nodes that are within its

Corresponding Author: Ramesh Ponnusamy, Department of Computer Technology, Anna University, Chennai, India

radio range). This value is a measure of the level of trust it has on its neighbour. The trust value is calculated using only local information. But the direct trust value is calculated as ratio of the number of packets forwarded to the number of packets to be forwarded. The negative observations about a node which is the number of packets dropped by it is not considered for calculation of direct trust. The negative observations about a node play a crucial role in determining the trust and are therefore incorporated in our approach. Moreover, there is no mechanism to filter out the dishonest recommendations during the calculation of indirect trust although it involves gathering trust value from multiple nodes. A filtering algorithm, carried out by the trust value cluster manager component ensures a more accurate indirect trust value in our approach.

Venkataraman *et al.* (2012) proposed a trust model where trust establishment and computation is divided into 3 phases: trust evidence collection, trust computation and choosing an optimal path with trust. Unlike the other models that considers only forwarding and dropping behavior of the nodes, few approaches take into account multiple trust metrics. While the cross layer approach proposed by Patil and Thorata (2013) considered observation, uncertainty, experience, recommendation and correctness of recommendation for trust value calculation of a node, the regression based trust model proposed by Venkataraman *et al.* (2012) used trust metrics that takes into account different behavior like willingness to participate in routing data forwarding, sincerity of the neighbouring nodes in forwarding the data without modification and these were stored as a trust vector for each neighbouring node. The 6 groups of data namely communication, data, recommendation, location, energy and cryptographic correctness were observed in the network for trust calculation by Geetha and Chandrasekaran (2014). In addition remaining battery power and stability factor of a node were also considered as important parameters for trust calculation.

Research on the subject of trust propagation in ad hoc networks has been extensively studied and various light weight mechanisms have been proposed to propagate the trust score. Since, ad hoc devices are sensor based resource constraint devices, lightweight trust vibration mechanism for trust propagation, trust accumulation and trust aggregation were integrated for resource constraint ad hoc networks. In order to ensure secure propagation of trust values, threshold cryptography was implemented in the network. Reduced overhead and overhead and faster completion of the authentication process was achieved. Bijon *et al.* (2014) presented a novel multi-hop recommendation based Trust Management Scheme (TRUISM) which adapted the Dempster Shafer Theory (Yang *et al.*, 2014) to efficiently combine recommendations from multiple devices in the presence of unreliable and malicious recommendations. TRUISM also provided a flexible behavioral model for trust computation where a node can prioritize recommendations based on its requirements.

Some other works on trust management and trust based routing were presented by Govindan and Mohapatra (2012), Umarani and Sundaram (2013), Peethambaran and Jayasudha (2014) and Kukreja *et al.* (2013) in which a detailed survey on various trust computing approaches that are geared towards MANETs are also discussed. They surveyed different properties of trust like context dependency, asymmetricity, transitivity, etc and presented cluster based and maturity based trust schemes. While Umarani and Sundaram (2013) discussed the general structure, design issues, trust metrics and the corresponding attacks and defense mechanisms of trust model, Peethambaran and Jayasudha (2014) discussed different kinds of attacks on MANETs and some protection mechanisms against those attacks. A comparison of these mechanisms was also included.

MATERIALS AND METHODS

Proposed work: A recommendation based trust model, which ensures secure transmission of packets from source to destination is proposed in this study. It consists of 5 components a trust quantifier component that computes direct as well as indirect trust; a dwindle applier that reduces the influence of past experience on the computed trust value; recommendation intermediary component that requests and gathers recommendations for a node from a list of recommenders and an outlier detector component which filters out dishonest recommendations from the list.

Trust quantifier component: Via. this component, each node observes its neighbours and constructs trust relationship which is the degree of belief that it can place on the neighbour (Govindan and Mohapatra, 2013). It is computed by accumulating the number of packets forwarded and dropped by each node which constitutes positive and negative observations, respectively (Zhang *et al.*, 2014). Each node maintains a data structure that contains each of its neighbour node's id, number of packets forwarded, dropped and trust value. Initially, trust that each node has on its neighbour is 1 indicating the absence of prior observation or interaction. Each node increments F-value of a neighbour every time a positive observation is made about the corresponding node. Similarly the d value is updated. The trust value is computed before forwarding a packet to a node to decide whether to forward to that neighbour or not.

Direct trust: If two nodes have communicated earlier, then they are aware of each other's behavior, making it possible for them to calculate the direct trust value. These nodes can continue to receive and forward each other's packet as long as there are in the same range. Direct trust that node i has on its neighbour j is calculated using the two parameters f and d as given in Eq. 1:

$$\text{Direct trust } T_{d(i,\ j)} = f/(f+d) \quad (1)$$

However, the direct trust value is not always acceptable as assumed in previous literature because nature of the nodes is dynamic. A legitimate node may turn malicious after some time or vice versa. There is also a possibility that the malicious behavior is targeted towards specific nodes. So in this model, after direct trust has been calculated for 3 times, recommendation from other nodes is used to evaluate the trust, i.e., indirect trust is evaluated.

Indirect trust: When two nodes have not communicated earlier or the number of interactions is less, it is not possible to calculate the trust value based on packet exchange between them. Such a situations demands the need for indirect trust value which is calculated based on the recommendations collected from neigbours. Indirect rust value is also calculated when the direct trust has been calculated multiple times, for reasons discussed earlier. However, malicious nodes may modify the trust value propagated in the network or generate dishonest recommendations. Thus, the following two components are incorporated to mitigate the influence of dishonest recommendations.

Recommendation intermediary component: The recommendation intermediary component that is present in each node is in charge of trust propagation. It broadcasts recommendation request to the evaluating node's neighbours, receives the set of recommendations from all the neighbours and sends them to the outlier detector to eliminate dishonest recommendations. In order to prevent the malicious nodes from modifying the trust values propagated by the neighbours, the trust values are encrypted using light weight encryption scheme proposed by Zhang *et al.* (2014). This ensures the safe propagation of trust values for indirect trust computation by preventing malicious nodes from modifying the trust values propagated by other nodes.

Algorithm 1:

1 For every indirect trust calculation,
2 Send recommendation request (rec_req) to neighbours
3 Collect the encrypted recommendations (trust values) from the neighbours
4 Decrypt the recommendations (trust values)
5 Construct T= $\{t_1, t_2, t_3 \ldots t_n\}$
6 Send T to outlier detector for processing
7 Receive dishonest recommendation class from outlier detector
8 Construct trustworthy cluster
9 End for

Outlier detector component: In this study, outlier refers to one or more trust values from the recommendation set R which is not consistent with the other recommendations, indicating its origin from a statistical distribution different from the remaining trust values. The outlier detector component receives a list of recommendations from the recommendation intermediary and processes it through the algorithm (Fig. 1).

Algorithm 2:

Input: set of trust values recommended by neighbours of evaluating node i about the evaluated node j.

i.e., T = { t_1, t_2, t_3, …, tn} where n is the number of recommendations. Output: t, aggregated trust value of evaluating node I about evaluated node j.

Place each trust value ti (i varies from 1 to n) in the appropriate interval $T_{ij}k$ (k lies within 1 to 10 range)

/* trust value, value lies between 0 and 1

Consider 10 intervals such that each interval contains values in the following range $T_{ij}1$ [0 0.1], $T_{ij}2$[0.1 0.2], $T_{ij}3$[0.2 0.3], $T_{ij}4$[0.3 0.4],….. $T_{ij}10$[0.9 1]

$T_{interval}$={ $T_{ij}1$, $T_{ij}2$, $T_{ij}3$, ... $T_{ij}10$}

*/

For x= 1 to 10 do

$T_{ij}x$= x/10

Find cardinality $C(T_{ij}x)$ for each interval $T_{ij}x$ (x varies from 1 to 10) If ($C(T_{ij}x)$ = = 0 for any x value)

Eliminate $T_{ij}x$ from $T_{interval}$ and obtained refined $T_{interval}$ Find discrepancy value for each interval Discrepancy($T_{ij}x$) = ($T_{ij}x$ – median ($T_{interval}$) $|^2$) / $C(T_{ij}x)$

$^{Sort\ T}$interval in descending order with respect to discrepancy value.

Construct $ST_{interval}$ which is initially empty

STinterval(x) = STinterval(x-1) ∪ Tijx where x = 1, 2, 3…m-1 and m is the distinct

recommendation n class value number in sorted in Tinterval.

Compute smoothing factor of $ST_{interval}$

SF(STinterval(x)) = C(Tinterval.-STinterval)*(DF(Tinterval)-DF(STinterval(x))) Return $St_{interval(x)}$ with the largest smoothing factor

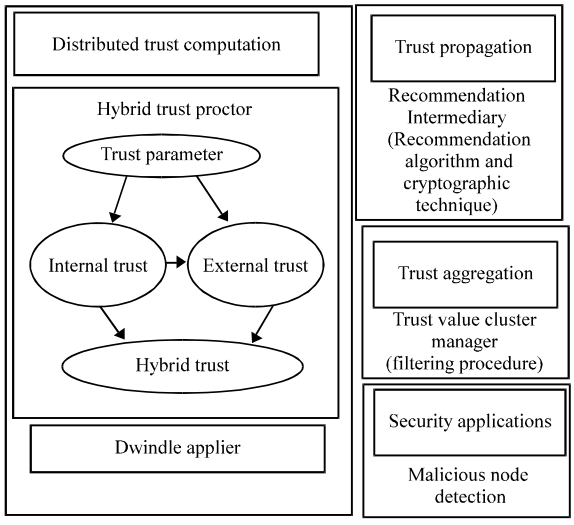

Fig. 1: Architecture diagram

$$\text{Discrepancy}(r)=\left(|r\text{-median}\left(T_{ij}x\right)|^2\right)/C\left(T_{ij}x\right) \quad (2)$$

The numerator of the above equation is known as median absolute deviation and it is not affected by the presence of outliers. T_r is sorted with respect to discrepancy value in descending order. To find the dishonest recommendation intervals from T_r smoothing factor which indicates the extent to which the discrepancy can be minimized is computed (Jichkar and Chandak, 2014). Smoothing Factor (SF) for each ST_r is computed as $SF(ST_r j) = C(T_r - ST_r(j))\times(\text{Discrepancy }(T_r)\text{-Discrepancy }(ST_r(j)))$ where j = 1, 2, 3, ..., m where m is the total number of distinct elements in ST_r. If $T_{ij}x$ is the xth recommendation interval of T_r and St_r is the set of suspicious recommendation intervals from T_r, $ST_r(x)$ which is initially empty can be constructed as $ST_r(x\text{-}1)$ $T_{ij}x$ where x = 1, 2, 3, .. m-1. The smoothing factor of, $ST_r(x)$ is computed. The subset, St_r (x) with largest smoothing factor is considered as a set containing dishonest recommendation.

Dwindle applier: Since, the nodes are mobile and the network environment is changing continuously, the influence of past experiences changes over time. The proposed trust model considers this influence by using the dwindle applier component. Before aggregating the newly computed trust values with the old ones, this component incorporates a decay factor to gradually decrease the influence of past experience over time. In most of the existing models, the influence of past experience is decreased when positive or negative experiences are observed with the interacting node. However, it is important to decay trust over time even without new positive or negative observations between the interacting nodes. If T_{i2} is trust value of node I at time t_2 and T_{i1} is trust value of node i at time t_1, then time dependent trust value (Jichkar and Chandak, 2014) is calculated using Eq. 2 (Fig. 2 and 3).

$$T_{i2} = T_{i1}\text{-}\left(0.002\times\left(t_2\text{-}t_1\right)\right) \quad (3)$$

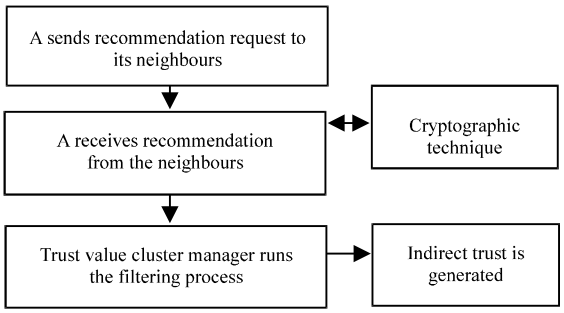

Fig. 2: Indirect trust computation

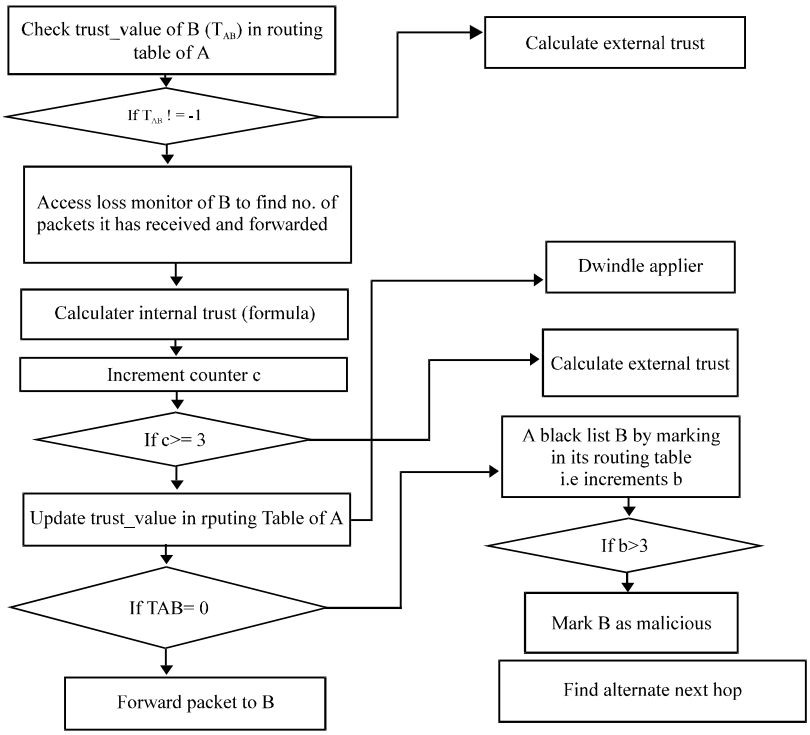

Fig. 3: Indirect trust computation

In the proposed model, when node A receives a packet for forwarding and node B is selected as the next hop, the sequence of steps depicted in the flow chart occurs. The trust that node A has on B (T_{AB}) is checked. Initially the trust value of every neighbour is -1. Every time the trust value is calculated, it lies between 0 and 1. So a trust value of -1 indicates that the node has not calculated the trust value earlier, indicating absence of communication with that neighbour.

If Tab is = -1, then indirect trust can be calculated directly. Otherwise, the loss monitor of B must be accessed to find the number of packets it has received and forwarded. Using these trust parameters, the direct trust value can be calculated and counter must be incremented. If the counter value is greater than or = 3, direct trust calculation must be followed by indirect trust calculation since there is a possibility that the trust value is not genuine. Repeated calculation of the direct trust value alone without including the recommendations of the neigbours results in false trust value being retained if a intruder exhibits malicious behavior selectively. In order to achieve this, recommendation intermediary of A requests recommendation about B to all its neighbours. Once the recommendations are received and filtered using filtering algorithm performed by trust value cluster manager, the direct and indirect trust value can be combined to quantify the hybrid trust value. If the computed trust value is 0, then A blacklists B by marking in its routing table. Similar to the technique used in (Laxmi *et al*., 2015) to detect jellyfish attack, if it has been marked >3 times then B is marked malicious in the routing table. Otherwise alternate next hop must be found.

RESULTS AND DISCUSSION

Simulation was carried out in a network with 20 randomly placed nodes in an area of 1000×1000 m. The parameters that were used in configuring the parameters is given in (Table 1). The performance of the proposed model is validated by measuring the network throughput and packet drop ratio in the presence of malicious nodes. The performance of the proposed model is validated by measuring the network throughput and packet drop ratio in the presence of malicious nodes. The nodes that recommend dishonest trust values are called dishonest recommendation nodes and such malicious nodes are included in the network and the throughput is measured of the network is measured. Then, the percentage of malicious nodes in the network is gradually increased and the network throughput is noted at each step. The values obtained after simulation of above scenario is shown in Table 2.

Figure 4 shows the effect of the presence of malicious nodes on the throughput of the network. The x-axis shows the percentage of malicious nodes in the network which is varied from 10-70% of the total population of the network and y axis shows the corresponding throughput. In the absence of efficient mechanism, the throughput which is initially around 80% deteriorates as the number of malicious nodes increases in the network. It finally drops to around 10% when the percentage of malicious nodes reaches 70% of the total population of the network. But the implementation of the trust model ensures a stable throughput even in the presence of malicious nodes. This indicates that an efficient mechanism can mitigate the influence of dishonest recommendation nodes in the network. Similarly the packet drop ratio is measured for varying number of malicious nodes. Without a defense scheme, the packet drop ratio increases considerably as the number of malicious nodes increases as indicated in (Fig. 4). The packet drop ratio is lower even

Table 1: Network configuration parameters

Parameters	Values
Simulation area	1000×1000 m
Node speed	5 m/sec
Queue length	50
Routing protocol	AODV
Mobility model	Radio propagation
Transmission range	250 m
No of mobile nodes	20
Routing protocol	AODV

Table 2:Performance measure of the network

Dishonest recommendation node (%)	Throughput		Packet drop ratio	
	With defense	Without defense	With defense	Without defense
0	0.794	0.794	0.20	0.20
10	0.788	0.602	0.21	0.30
20	0.795	0.511	0.25	0.44
30	0.790	0.421	0.25	0.50
40	0.777	0.300	0.25	0.60
50	0.776	0.202	0.25	0.76
60	0.775	0.220	0.25	0.80
70	0.770	0.101	0.25	0.90

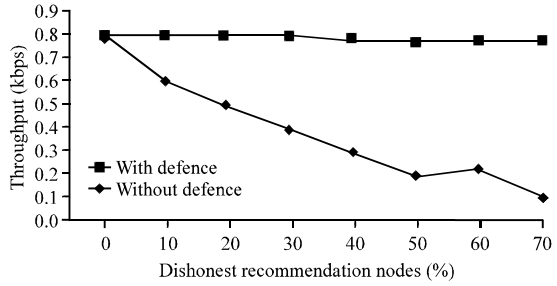

Fig. 4: Throughput vs. percentage of dishonest recommendation nodes

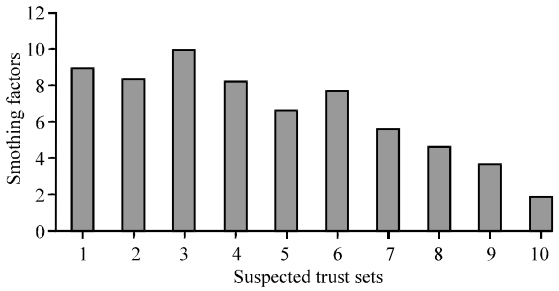

Fig. 5: Detection of bad mouthing attack

in the presence of malicious nodes as nodes avoid packet propagation through them. In bad mouthing attack, an attacker share low trust values about an entity as recommendation for decreasing trustworthiness of the entity. For bad mouthing attack we have considered Three scenarios: 10% dishonest recommenders, 30% dishonest recommenders and 60% dishonest recommend Fig. 5 shows the scenario of 10% dishonest recommenders in which 10% of the bad mouthers are low trust worthy and high values in the set containing 0.2 and 0.10 are detected as disconnect recommendations.

In ballot stuffing attack, an attacker share high trust values about an entity as recommendation for elevating trustworthiness of the entity. For ballot stuffing attack we have considered three scenarios: 10% dishonest recommenders, 30% dishonest recommenders and 60% dishonest recommenders. In Fig 6 shows the set 2 containing the highest trust value is consider as the dishonest recommender. In Fig. 7 shows results for bad-mouthing attack while y-axis shows the proportion of the recognized dishonest recommendation, false negative and false positive with the defence scheme in action. It can be observed theat the defence algorithm can effectively mitigate the dishonest recommendations.

In Fig. 8 is obvious when there is no defence incorporated the proportion of recognition drops-stuffing attackers from about 9 to nearly 1 with variation of the

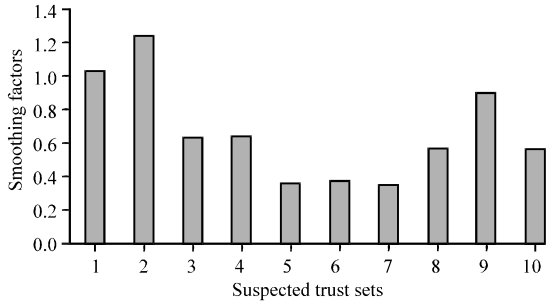

Fig. 6: Suspated trust sets of ballot stuffing attack

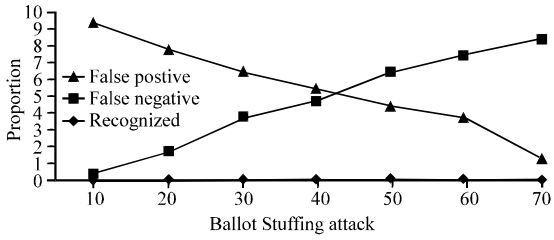

Fig. 7: Detection of bad mouthing attack

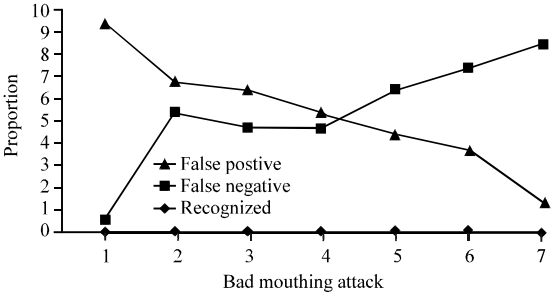

Fig. 8: Detection of ballot stuffing attack

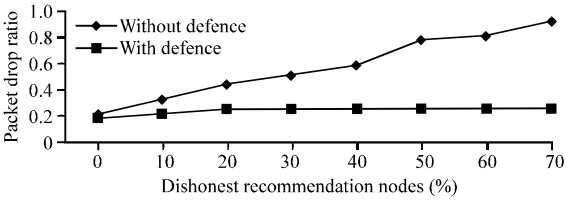

Fig. 9: Packet drop ratio vs. percentage of dishonest recommendation nodes

ballot-stuffing attackers from 1-8. The false negative proportion also increases to nearly 9 with the increasing percentage of the dishonest recommending nodes. Figure 9 shows the comparison of the trust values under three different cases. The x-axis shows the percentage of bad-mouthing attacker nodes and y-axis shows a specific node's trust value. The trust value of the node in the absence of malicious nodes is the expected value of trust.

Table 3: Effect of bad mouthing attack on trust value of nodes

Bad mouthing attack node	10%			30%			60%		
Node No.	EV	With out defense	With defense	EV	With out defense	With defense	EV	With out defense	With defense
1	0.84	0.76	0.838	0.88	0.70	0.880	0.850	0.75	0.850
2	0.74	0.69	0.730	0.79	0.65	0.800	0.720	0.54	0.720
3	0.69	0.57	0.650	0.50	0.56	0.540	0.600	0.45	0.600
4	0.78	0.60	0.780	0.89	0.78	0.900	0.750	0.67	0.744
5	0.05	0.02	0.050	0.13	0.04	0.130	0.150	0.06	0.150
6	0.43	0.39	0.400	0.56	0.45	0.567	0.560	0.40	0.560
7	0.79	0.51	0.750	0.81	0.67	0.810	0.840	0.74	0.840
8	0.81	0.62	0.800	0.90	0.50	0.890	0.760	0.59	0.760
9	0.02	0.01	0.020	0.14	0.01	0.140	0.230	0.19	0.230
10	0.87	0.54	0.860	0.78	0.60	0.780	0.744	0.65	0.750
11	0.39	0.12	0.380	0.54	0.38	0.540	0.630	0.45	0.630
12	0.01	0.00	0.010	0.15	0.09	0.150	0.180	0.08	0.180
13	0.27	0.13	0.250	0.35	0.24	0.350	0.490	0.33	0.490
14	0.69	0.49	0.670	0.78	0.56	0.780	0.830	0.77	0.830
15	0.95	0.78	0.910	0.95	0.60	0.920	0.950	0.35	0.920

Table 4: Effect of ballot stuffing attack on trust value of nodes

Ballot mouthing attack node	10%			30%			60%		
Node No.	EV	With out defense	With defense	EV	With out defense	With defense	EV	With out defense	With defense
1	0.690	0.76	0.690	0.530	0.72	0.530	0.46	0.74	0.460
2	0.520	0.74	0.520	0.670	0.70	0.670	0.56	0.69	0.560
3	0.350	0.49	0.350	0.430	0.50	0.430	0.31	0.54	0.320
4	0.680	0.78	0.680	0.540	0.74	0.540	0.45	0.80	0.450
5	0.090	0.15	0.090	0.110	0.17	0.110	0.12	0.20	0.120
6	0.470	0.56	0.470	0.450	0.52	0.450	0.33	0.49	0.330
7	0.660	0.76	0.660	0.540	0.78	0.540	0.43	0.75	0.430
8	0.810	0.62	0.810	0.480	0.67	0.477	0.35	0.69	0.350
9	0.005	0.01	0.005	0.001	0.03	0.001	0.01	0.07	0.010
10	0.770	0.86	0.760	0.730	0.82	0.730	0.57	0.89	0.570
11	0.250	0.39	0.250	0.250	0.43	0.250	0.25	0.45	0.250
12	0.100	0.12	0.100	0.090	0.15	0.090	0.02	0.18	0.020
13	0.190	0.25	0.190	0.210	0.27	0.210	0.16	0.29	0.150
14	0.570	0.69	0.570	0.550	0.72	0.550	0.43	0.76	0.430
15	0.150	0.78	0.910	0.156	0.20	0.156	0.15	0.45	0.156

The expected value of node 15 is recorded. Then few malicious nodes were introduced in the network and the trust value of the node was recorded. In the presence of malicious nodes, the trust value is wrongly recommended resulting in a vast variation from the expected value. Then trust value of the same node is recorded after implementation of the proposed trust recommender model. The elimination of dishonest recommendations by the recommender model results in the trust value that is consistent with the expected value. Similar results are obtained in the presence of ballot-stuffing attackers as shown in Fig. 10 and 11. The values recorded after simulation of the above mentioned scenarios are show in Table 3 and 4.

The performance of the proposed model is compared with model by Umarani and Sundaram (2013) using trust level error which represents the proportion of error during trust evaluation of a node. The graph in (Fig. 12) shows the effectiveness of our model in minimizing the trust level error. During the entire period of evaluation, the trust level error is consistent in the proposed model.

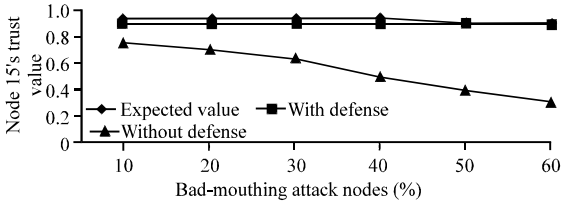

Fig. 10: Node 15's trust value vs. bad-mouthing attack percentage

Mobile ad hoc network is characterized by constrained resources interms of communication, memory, power usage, computational complexity requirements. Any proposed model must reflect the tradeoffs between accuracy of trust worthiness and performance of network. As gathering and propagating trust information among distributed nodes can consume more resources of energy and time, it can enhance decision making. Dynamic and highly mobile network which suffer from several points of failure require techniques to enhance decision making on node trust worthiness. However, the proposed model

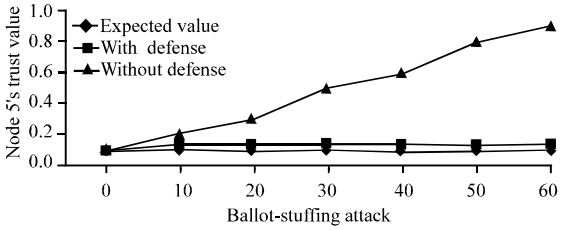

Fig. 11: Node 15's trust value vs. ballot-stuffing attack percentage

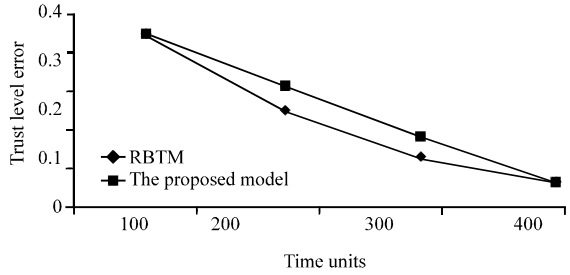

Fig. 12: Trust level error vs. time units

is light weight in several aspects. The packets of recommendation are exchanged between single source of information which is represented in the recommendation intermediary component to and from the evaluating node and evaluating nodes. The data size and length is very small as every recommending node provides only three parameters of accumulated positive and negative information which are completely protected via. demand scheme in which recommendation can be requested whenever needed. Therefore, the model is conducted is conducted without network flooding and acquisition delay.

CONCLUSION

A complete trust-based recommendation model for MANET, involving various aspects of trust like trust computation, propagation, aggregation is proposed and evaluated to deal with attacks related to dishonest recommendations. The recommendation intermediary component incorporates encryption and statistical approach based filtering algorithm to overcome the problems of false recommendations during trust propagation and aggregation. The results obtained after implementation of the proposed model indicated improved consistency of received recommendations and consequently decrease in the the influence of false estimations on trust computation.

SUGGESTIONS

Our future research is concentrated on improving this model to work efficiently in a network that is prone to other attacks. The model can be extended by weighting recommenders based on time and location of receiving these recommendations to mitigate the influence of location and time dependent attacks (recommending nodes differently according to time and location).

REFERENCES

Bijon, K.Z., M.M. Haque and R. Hasan, 2014. A trust based information sharing model (TRUISM) in MANET in the presence of uncertainty. Proceedings of the 12th Annual International Conference on Privacy, Security and Trust (PST) 2014, July 23-24, 2014, IEEE, San Antonio, Texas, ISBN:978-1-4799-3504-8, pp: 347-354.

Biswas, S., T. Nag and S. Neogy, 2014. Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET. Proceedings of the 2014 Conference on Applications and Innovations in Mobile Computing (AIMoC), February 27-March 1, 2014, IEEE, Kolkata, India, ISBN:978-1-4799-3881-0, pp: 157-164.

Geetha, V. and K. Chandrasekaran, 2014. A distributed trust based secure communication framework for wireless sensor network. Wirel. Sens. Netw., 6: 173-183.

Govindan, K. and P. Mohapatra, 2012. Trust computations and trust dynamics in mobile adhoc networks: A survey. Commun. Surv. Tutorials, 14: 279-298.

Jichkar, M.R.A. and M.B. Chandak, 2014. Application of indirect trust computation in MANET. Intl. J. Adv. Res. Comput. Commun. Eng., 3: 5819-5826.

Kukreja, D., U. Singh and B.V.R. Reddy, 2013. A survey of trust based routing protocols in MANETs. J. Adv. Comput. Netw., 1: 280-285.

Kumar, A., K. Gopal and A. Aggarwal, 2013. Lightweight trust propagation scheme for resource constraint mobile ad-hoc networks (MANETs). Proceedings of the 6th International Conference on Contemporary Computing (IC3) 2013, August 8-10, 2013, IEEE, Noida, India, ISBN:978-1-4799-0191-3, pp: 421-426.

Laxmi, V., C. Lal, M.S. Gaur and D. Mehta, 2015. JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. J. Inf. Secur. Appl., 22: 99-112.

Marchang, N. and R. Datta, 2012. Light-weight trust-based routing protocol for mobile ad hoc networks. IET. Inf. Secur., 6: 77-83.

Patil, V.N. and S.A. Thorat, 2013. Cross layer approach to detect malicious node in MANET. Proceedings of the 4th International Conference on Computing Communications and Networking Technologies (ICCCNT) 2013, July 4-6, 2013, IEEE, India, ISBN:978-1-4799-3925-1, pp: 1-6.

Peethambaran, P. and J.S. Jayasudha, 2014. Survey of manet misbehaviour detection approaches. Intl. J. Network Secur. Appl., 6: 19-29.

Shabut, A.M., K.P. Dahal, S.K. Bista and I.U. Awan, 2015. Recommendation based trust model with an effective defence scheme for MANETs. IEEE. Trans. Mobile Comput., 14: 2101-2115.

Shakshuki, E.M., N. Kang and T.R. Sheltami, 2013. Eaack: A secure intrusion-detection system for Manets. IEEE. Trans. Ind. Electron., 60: 1089-1089.

Umarani, V. and K.S. Sundaram, 2013. Survey of various trust models and their behavior in wireless sensor networks. Intl. J. Emerging Technol. Adv. Eng., 3: 180-188.

Venkataraman, R., M. Pushpalatha and T.R. Rao, 2012. Regression-based trust model for mobile ad hoc networks. IET. Inf. Secur., 6: 131-140.

Yang, B., R. Yamamoto and Y. Tanaka, 2014. Dempster-shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETS. Proceedings of the 16th International Conference on Advanced Communication Technology (ICACT) 2014, February 16-19, 2014, IEEE, Tokyo, Japan, ISBN:978-1-4799-3217-7, pp: 223-232.

Zhang, P., C. Lin, Y. Jiang, Y. Fan and X. Shen, 2014. A lightweight encryption scheme for network-coded mobile ad hoc networks. IEEE. Trans. Parallel Distrib. Syst., 25: 2211-2221.