Indian Journal of Science and Technology, *Vol 9(4), DOI: 10.17485/ijst/2016/v9i4/87043, January 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Enhancing the Security for Manet by Identifying Untrusted Nodes using Uncertainity Rules

S. Muthuramalingam* and T. Suba Nachiar

Department of Information Technology, Thiagarajar College of Engineering, Madurai - 625005, Tamil Nadu, India; smrit@tce.edu, subhanatchiar.t@gmail.com

Abstract

Background/Objectives: Trust based models offer security against vulnerabilities due to the dynamic and open wireless medium. The raise up of uncertain reasoning methods originates from the artificial intelligence leads to trust management protocols for the creation of secure environment in MANET. **Methods/Statistical Analysis**: In this paper, two schemes namely, direct and indirect observation based trust evaluation are proposed. Initially, the network is formed to investigate the security. The utilization of full probability model in Bayesian interface evaluates the trust from the observer node in direct observation scheme. Alternatively, the neighbor hop information is used in the derivation of trust value in indirect observation scheme. Another type of uncertain reasoning called Dempster-Shafter theory calculates the trust value after the observation schemes. Finally, the Dijkstra's algorithm establishes the routing process on the basis of shortest path. **Findings**: The proposed observation schemes provide more accurate results compared to existing ones. The comparative analysis of proposed hybrid model with the existing model assures the effectiveness on the parameters of Packet Delivery Ratio (PDR), throughput with less overhead for variation in number of nodes and node speed. **Improvements/Applications:** The results of MANET routing scenario positively support the effectiveness and performance of our scheme and we can extend the proposed scheme to MANETs with cognitive radios.

Keywords: Bayesian Interface, Dempster-Shafter Theory (DST), Direct Observation, Indirect Observation, Mobile Ad-hoc Network (MANET), Security, Trust Evaluation, Uncertain Reasoning

1. Introduction

Trust management in Mobile Adhoc Network (MANET) is considered as the challenging task to achieve the various issues such as reliability, reconfigurability and scalability. The resource constraints based operations and dynamic operation are considered to govern the interactions of MANET with cognitive, communication. The multi-hop communication in MANET without centralized architecture affected by the security vulnerabilities. Node trust models and data trust models are evolved in research works enhances the security performance against malicious attacks. Traditional research works lists the classification trust management schemes, merits and the potential risks under the multi-disciplinary concept.

The distinct features of MANET such as loss of centralized architecture, distributed and open wireless medium raises the potential risks in data transfer. Hence, security is one of the important parameters in the design of MANET. The increase in real world deployment of MANET models motivate the Optimized Link State Routing (OLSR) into new version as OLSRv2 in which three processes are embedded namely, neighborhood discovery, MPR flooding and link state advertisement. The focus of trust management scheme to detect the malicious behavior of nodes to preserve the reliability in OLSRv2.

The trust based Ad-hoc On Demand Vector (AODV) track, isolates the misbehaving nodes from the routing process. One of the dynamic trust computational models termed as *Secured Trust* investigates the different factors

*Author for correspondence

required to evaluate the trust. The establishment of the most trust routes rather than the shortest path to make the better utilization of MANET in hostile environment. The consumption of limited computational resources leads to creation of light weight trust protocols.

Continuous user authentication is an important prevention based approach to offer the protection to high security MANETs. Also, the identification of malicious activities also important challenge. The inclusion of security and resource constraints handles the above mentioned functions jointly by Partial Observable Markov Decision Processes (POMDP). The authentication and topology control are performed separately in the existing works offers the minimum throughput. To overcome this problem, joint topology control and authentication are proposed in research work in accordance with channel and relay conditions. The nodes with selected features of node reputation and identity information in friendship mechanism extends the traditional AODV protocol to FrAODV for the evaluation of routing paths. Based on trust factor in initialization phase and the updating of trust value in route exchanging process yields the better results of Packet Delivery Ratio (PDR), throughput. The equal treatment of malicious and faulty behaviors provided the maximum overhead. To minimize the overhead, Context-Aware Security and Trust Frame work effectively separates the malicious behaviors from faulty behaviors. The integration of cognitive networks with the MANET (CR-MANET) offers many security problems. The evolution of mean game theoretic approach deals with the security problems to enable the individual node to make the strategic decisions. The interaction of multi-agents in CR-MANET provides the required security assurance. Hence, a Hierarchical and Bayesian Inferred Trust (HABIT) in research works assures how the agents should trust peers with direct and third party information. The conventional methods provided the best secure performance against black hole attack. But, they may fail to detect the gray-hole attacks. To handle this problem, Dempster-Shafter evidence based trust management theory is introduced. From the study, it is observed that, trust management based on indirect observation scheme used reliability of nodes which are not in the ranges of observer node and in direct observation scheme do not differentiate the data and control packets. Hence, inaccurate trust values are derived. In this paper, interpretation and recognition of trust with direct and indirect observation are discussed to create the secure MANET environment.

The technical contributions of proposed hybrid observation model compared to traditional models are listed as follows:

- The proposal of unified trust management based on uncertain reasoning to enhance the security of MANET.
- The achievement of differentiation of data and control packets.
- Extensive simulation study of implementation of proposed observation scheme in OLSRv2 confirms the effectiveness on packet delivery ratio and throughput.

This section describes the traditional trust management schemes in MANET and the associated types, merits and limitations that leads to proposed hybrid observation model. Trust management in MANET is the challenging task due to the existence of critical co-operation among the devices. [1]Discussed the concepts of trusts and derived the unique characteristics of trust. They surveyed the trust management schemes in MANET and discussed the classifications, attacks and metrics. WSN are susceptible to various security threats because of delay constraints. [2]Presented the survey of trust models applied to WSN. They analyzed the various applications of trust models such as malicious attack detection, secure routing and data aggregation. The independent movement of nodes and computational complexities made the trust computation as challenging one. [3]Presented the detailed survey of trust computing approaches and the comparisons between them. They analyzed various works on trust dynamics. The preservation of MANET connectivity was an investigating parameter when they faced the malicious participants. [4]Reviewed the algorithms to construct the Optimized Link State Routing Protocol v2 (OLSRv2) identifies the vulnerabilities and how the protection was improved against the attacks raised. The observational shortcomings were addressed in uni-modal bio-metric systems where the continuous user-to-device authentication achieved. [5]Studied the distribution of combined authentication and Intrusion Detection Systems (IDS) to eradicate the shortcomings. The decision about whether the user authentication is required or devices are chosen was made on distributed manner.

[6]Formulize the combined user-authentication with IDS problem by using Partial Observable Markov Decision Process (POMDP). They solved the problem by the structural results of large network that contains various nodes. The failure occurs in prediction of trust value

due to unpredictable way of malicious behavior nodes. [7]Presented the dynamic trust computational model called *Secured Trust* which analyzed the factors affecting the trust evaluation and presented the quantifying model for measurement of trust. In traditional models, authentication and topology control are carried out in separate manner. [8]Jointly considered the authentication and topology control models on the basis of channel and relay conditions. They improved the throughput by using Joint Authentication and Topology Control (JATC). The ultimate aim of design of MANET is to support the co-operative environment. The establishment of most trust nodes rather than shortest path nodes constituted the MANET environment to offer the trust. [9]Presented the light-weight trust based routing protocol which consumes less resources for trust computation. The computation requires the local information that offers the scalability. The node misbehavior due to the malicious action significantly degraded the performance of MANET. Moreover, the QoS parameters such as Packet Delivery Ratio (PDR), throughput and delay were affected by the malicious nodes. [10]Presented the Trust Based Reliable AODV (TBRAODV) which calculates the trust value for each node. Based on the trust value, either nodes are participated in the routing or they are identified as malicious nodes. The reliability of TBRAODV based system was increased. [11]Presented a reactive protocol namely, Distributed Dynamic Source Routing (D-DSR). It Slows down the attacker from copying the response of the packets. A multi-path secured routing scheme is used to attain the secured network. The consistency and performance of the protocol is measured through attack prevention efficiency, PDR, routing packet overhead and path optimality. It provides high security .

The analysis of malicious traffic leads to provision of anonymous communications in MANET. [12]Proposed the Anonymous Overlay System (AOS) proved the strong source and destination based on strong adversary model. The traditional traffic analysis models in MANET equally treated the malicious and faulty behaviors. [13]Propose the study of Context Aware Security and Trust (CAST) framework utilized the contextual information such as status of channel and battery to isolate the malicious behavior from faulty one. The conversion of AODV into secured AODV achieved by the new mechanism called friendship mechanism. [14]Presented the FrAODV such that the node's friendship is evaluated by using some selected features. They calculated the routing path on the basis of selected features of node reputation and identity information. The situations of inconsistency and malicious nodes encounter raised in friendship mechanism. [15]Showed that how trust based reasoning model calculate the behavior of another node. Different simulation scenarios performed to protect the malicious nodes and preserve the behavioral results. The evaluation of behavioral patterns governed by agents which depends upon the reputation and trust mechanisms. [16]Illustrated the proliferation which trust and reputation are considered to offer the high level of security in MANET applications. Various types of attacks such as Black holes, Byzantine and rushing attacks made the trust based MANET as a challenging task.

[17]Presented the overview of trust management in MANET. The working principle depends upon trust factor in the initialization phase and the routing path establishment based on evaluated trust value during the routing exchange process. The selection of routing path depends upon various constraints such that all nodes in the routing path are trustworthy, non-malicious and unselfish. But, practically selfish or malicious nodes degraded the performance. [18]Found the path in which there is no selfish nodes was exist. They removed the low energy nodes in routing path. Security defense by the individual node in traditional trust based MANET consumed more number of resources. [19]Discussed the mean field game theoretic approach which not only consider the security. But, it also concerned the resources consumption with the large number of nodes were involved. The participated agents in MANET have the capability of knowing the reliable interaction partners. [20]Presented the theoretical and simulation background of Hierarchical and Bayesian Interface Trust (HABIT) which predicted the trust performance on the basis of multiple representations. The conventional methods offered the good performance only for black hole attack. [21]Discussed the Dempster-Shafter Theory (DST) in which neighborhood model was created on the basis of Watch dog mechanism and took the historical evidence by the DST evidence based trust management. The study of traditional methods conveyed that the simultaneous observation schemes are required to create the high secure environment.

2. Proposed Work

This section defines the proposed hybrid observation model (direct and indirect) based trust in MANET. The flow of proposed model is shown in Figure 1.

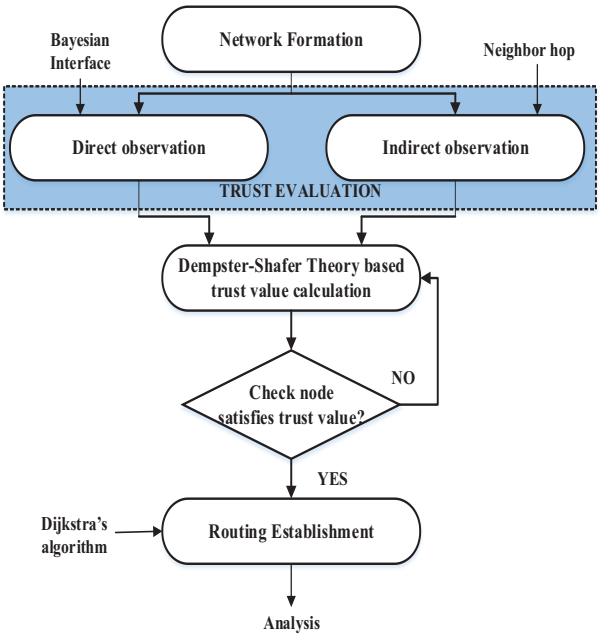

Figure 1. Overall flow of proposed hybrid observation model.

The model contains sequential processes network formation, direct observation and indirect observation based trust evaluation, Dempster-Shafter theory based trust value calculation and Dijkstra's algorithm based routing path establishment. In direct observation scheme, the uncertain reasoning model called Bayesian inference is used to calculate the trust value. The neighbor nodes of observer nodes are participated in the indirect observation scheme. The Dempster-Shafter Theory (DST) is applied to calculate the trust value. The minimization utilization in Dijkstra's algorithm established the routing path. The conversion of trust value into untrustworthy and the minimization of untrustworthy value achieved by using the Dijkstra's algorithm. The calculated trust values and the routing tables are stored in Trusted Platform Module (TPM). The trust values in each node are considered as key facilities for malicious node detection.

2.1 Network formation

The Mobile Ad-hoc Network (MANET) constructed using various components. They are Domain (D), Domain Router (DR), Co-Domain Router (CDR), Inter Domain Router (IDR), Client Router (CR), and Client Fringe (CF). Domain is the set of devices connected through the domain router. The DR performs various functions such as routing of messages to the specified clients, resolving of domain merging and forwarding of messages to the inter domain. The domain formation processed messages are limited by Co-Domain Router (CDR). The IDR acts as the gateway to the neighboring DR and clients. The member of each domain is identified by the CR. The CF is the device that has only one connection with the CR. The pictorial form of the network formation are shown in Figure 2.

The link stability and route lifetime are considered without overhead in the formation. Various parameters required for the initialization of network are area, number of nodes, transmission range and maximum speed of the node. The area defined the MANET environment as square with the dimensions of 870×870 m^2. The transmission range for the data packets be 250 units. The number of nodes varied from 50 to 100 in which the 20 nodes have the destination and the routing information top the destination. The maximum speed of the node is set as 10 m/sec and the maximum simulation time set it as 500 sec.

2.2 Direct Observation

The degree of belief for a node in network to carry the tasks referred as trust. The trust model comprises the following properties as follows:

- Subjectivity- The right of an observer node to compute the trust values
- Dynamicity – Changes in trust if the behavior of node changes.

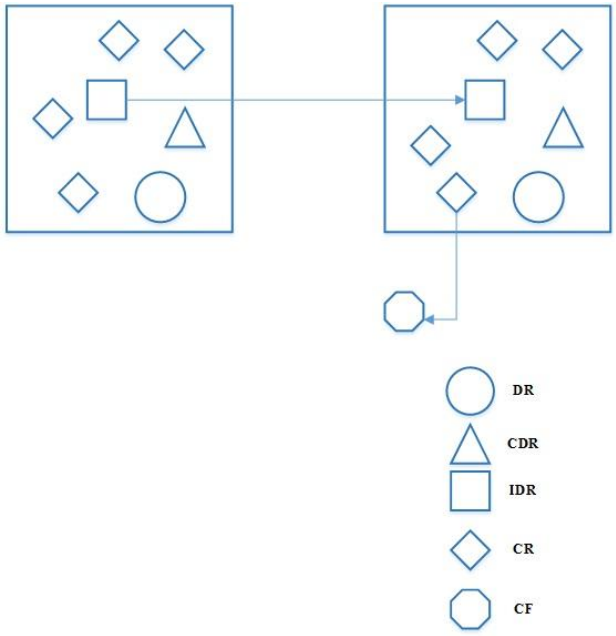

Figure 2. Network formation.

- Non-transitivity- The property is defined as follows: Node 1 trust the node 2 and Node 2 trust the Node 3. Then, the node 1 does not trust the Node 3.
- Asymmetry – Node 1 trust the Node 2. But the Node 2 does not trust the Node 1.
- Context dependence – Assessment of trust depends upon the behavior of nodes.

The evaluation of trust in proposed scheme is based on above mentioned properties and the obtained trust values lies in ranges of 0 and 1. The symbols used for trust evaluation in proposed system listed in Table 1.

The accurate trust value T of a node in MANET which includes the trust from direct observation T^S and trust from indirect observation T^N defined by,

$$T = \lambda T^S + (1-\lambda)T^N \tag{1}$$

The assumption to implement the direct observation is that, each observer overhead the packets and compared with the original packets to detect the malicious behavior. The reduction of estimation of unknown probability governed by Bayesian inference theorem described as

$$f(\theta,y\,|\,x) = \frac{p(x\,|\,\theta,y)f(\theta,y)}{\int_0^1 p(x\,|\,\theta,y)f(\theta,y)d\theta} \tag{2}$$

Here, x is the number of packets forwarded, y is the number of received packets, and $p(x\,|\,\theta,\ y)$ is the maximum likelihood function which follows the binomial distribution. The prior distribution function follows the Beta distribution as follows:

$$Beta(\theta;\alpha,\beta) = \frac{\theta^{\alpha-1}(1-\theta)^{\beta-1}}{\int_0^1 \theta^{\alpha-1}(1-\theta)^{\beta-1}d\theta} \tag{3}$$

The expectation of Beta function defined as follows:

$$E(Beta) = \frac{\alpha}{\alpha+\beta} \tag{4}$$

The inclusion of punishment factor in expectation function decreases the trust of an attacker when it misbehaves and the trust of an attacker will note recover quickly as follows:

$$E(Beta) = \frac{\alpha}{\alpha+\gamma B} \tag{5}$$

The trust value is calculated with direct observation is computed by

$$T^S = E(Beta) \tag{6}$$

Larger punishment factor declines the more trust since, the punishment factor assigns more weight to misbehavior nodes. The algorithm for direct observation contains various steps. Initially, Node A is an observer node and its one-hop neighbor trustee Node B. Then, the forwarding of packets takes place. If node A observes Node B forward the packet, then the number of packets forwarded increases to one and if the overflow occurs in Node B, then the number of packets received are decreases to one. Finally, calculate the trust value of node by using (6) and repeat the process. The direct observation algorithm is listed as follows:

Direct observation
Initialize node A as an observer node, *Rxcount* = 0, *Frcount* = 0.
Find one-hop neighbor to node A and set it as node B
If node B receives the packets
Increment *Rxcount* to one
If node B forward the packets
Increment *Frcount* to one
Else
If node B is overflow
Decrement *Rxcount* to one
End if
End if
End if
Calculate the trust T^S

Table 1. Symbols Used

Symbols	Description
T_{AH}	Trust value that Node A gives Node B
T_{AH}^S	Trust value that Node A gives Node B on the basis of direct observation
T_{AH}^N	Trust value that Node A gives Node B on the basis of indirect observation
T_{AH}^D	Trust value that Node A gives Node B on the basis of data packets
T_{AH}^C	Trust value that Node A gives Node B on the basis of control packets
λ	Weight for trust value based on direct observation
ρ	Weight for trust value based on data packets
ϒ	Punishment factor

2.3 Indirect Observation

The assumption to implement the indirect observation scheme is that more than one neighbor nodes between the observer and observed node. The neighbor nodes provided the evidence in independent nature. The discernment frame (Ω) theory is the basis for indirect observation. For a set (A_i) , the probability value is the function (m) satisfies the following conditions.

Condition 1: $m = 0$

Condition 2: $\sum_{A_i \subseteq \Omega} m(A_i) = 1$

Based on these conditions the belief function for the subset is defined as,

$$bel(B) = \sum_{A_i \subseteq B} m(A_i) \tag{7}$$

Let us consider the hypothesis H denotes the trustworthy, $\bar{H}$ denotes the untrustworthy and $U = \Omega$ describes whether the node is trust or untrustworthy. The basic probability value for each hypothesis between {0, 1}. The derivation of probability value depends upon two cases as follows:

Case I:

The node j_1 believes the node B is trustworthy. Then, the probability values derived by,

$$\left.\begin{aligned} m_{j_1}(H) &= T^S_{Aj_1} \\ m_{j_1}(\bar{H}) &= 0 \\ m_{j_1}(U) &= 1 - T^S_{Aj_1} \end{aligned}\right\} \tag{8}$$

Case II:

The node j_1 believes the node B is untrustworthy. Then, the probability values derived by,

$$\left.\begin{aligned} m_{j_1}(H) &= 0 \\ m_{j_1}(\bar{H}) &= T^S_{Aj_1} \\ m_{j_1}(U) &= 1 - T^S_{Aj_1} \end{aligned}\right\} \tag{9}$$

The corresponding belief function for the probability values derived as follows:

$$\left.\begin{aligned} bel_{j_1}(H) &= m_{j_1}(H) \\ bel_{j_1}(\bar{H}) &= m_{j_1}(\bar{H}) \\ bel_{j_1}(U) &= m_{j_1}(H) + m_{j_1}(\bar{H}) + m_{j_1}(U) \end{aligned}\right\} \tag{10}$$

From the testimonial function derived from (7) to (10) the trustworthy of node A derive the trustworthy of node B.

2.4 Dempster-Shafter Theory based Trust Evaluation

The Dempster-Shafter Theory (DST) is used for trust calculation. Let us consider the two belief functions of node B defined by $bel_1(B)$ and $bel_2(B)$ over discernment frame Ω. The orthogonal sum of belief function defined as follows:

$$\begin{aligned} bel(B) &= bel_1(B) \oplus bel_2(B) \\ &= \frac{\sum_{i,j,A_i \cap A_j = B} m_1(A_i) m_2(A_i)}{\sum_{i,j,A_i \cap A_j \neq \varnothing} m_1(A_i) m_2(A_i)} \end{aligned} \tag{11}$$

With the consideration of one-hop neighbors to the node B, the probability function are modified as follows:

$$\begin{aligned} & m_{j_1}(H) \oplus m_{j_2}(H) \\ &= \frac{1}{K}\left[m_{j_1}(H) m_{j_2}(H) + m_{j_1}(H) m_{j_2}(U) + m_{j_1}(U) m_{j_2}(H) \right] \\ & m_{j_1}(\bar{H}) \oplus m_{j_2}(\bar{H}) \\ &= \frac{1}{K}\left[m_{j_1}(\bar{H}) m_{j_2}(\bar{H}) + m_{j_1}(\bar{H}) m_{j_2}(U) + m_{j_1}(U) m_{j_2}(\bar{H}) \right] \\ & m_{j_1}(U) \oplus m_{j_2}(U) = \frac{1}{k}\left[m_{j_1}(U) + m_{j_2}(U) \right] \end{aligned} \tag{12}$$

From (11) and (12) the trust value based on indirect observation defined as follows:

$$T^N_{AB} = m_{j_1}(H) \oplus m_{j_2}(H) \ldots\ldots \oplus m_{j_n}(H) \tag{13}$$

The algorithm for trust calculation based on indirect observation as follows:

Indirect observation
Initialize node A as an observer node
Compute the one-hop neighbor nodes to node A
If *(one-hop>1)*
Calculate the trust value using equation (13)
Else
Set trust value as zero
End if

2.5 Security Routing Establishment

In traditional OLSRv2, the minimization is provided by Dijkstra's algorithm in such a way that, the shortest path is derived from the node with minimum hop count. To eval-

uate this, the trust value is converted into untrustworthy value. Then the minimization of untrustworthy by the Dijkstra's algorithm offers the secure routing in MANET. The untrustworthy values between nodes A and B is defined by

$$U_{AB} = 1 - T_{AB} \tag{14}$$

The sum of untrustworthy values for the path containing the nodes k_i and its one-hop neighbor nodes k_{i+1} described as follows:

$$U_{path} = \sum_{i=1}^{n-1} U_{k_i k_{i+1}} = \sum_{i=1}^{n-1} \left(1 - T_{k_i k_{i+1}}\right) \tag{15}$$

The best route is selected should satisfies the minimum of U_{path}. The calculated trust values and the updating routing paths are stored in Trusted Platform Module (TPM) offers the security to open wireless environments. The key parameter to detect the malicious nodes are the calculated trust values. Hence, the proposed scheme effectively separate the malicious behavior from the faulty behavior.

4. Results and Discussion

The proposed scheme is implemented on OLSRv2 protocol. During the simulations in NS 2, the effectiveness is validated in insecure environment. The comparative analysis of proposed trust observation scheme with the existing OLSRv2 without security mechanisms on the parameters of Packet Delivery Ratio (PDR), delay, throughput against the variation of mean node speed and number of malicious nodes.

4.1 Packet Delivery Ratio

The measure of number of packets delivered to the destination node against the number of packets generated by the source node termed as Packet Delivery Ratio (PDR). The analysis of PDR with the variation of mean node speed for proposed and existing OLSRv2 is depicted in Figure 3.

Figure 3 describes the relationship between PDR with the mean node speed for proposed and existing method. The trust based routing calculation effectively detect the malicious behavior. The trust with indirect and direct observation mechanism provided the high PDR compared to existing insecure OLSRv2.

4.2 Packet Delay

The measure of delay between packet transmissions from source node to destination node for the maximum traffic referred as packet delay. The analysis of packet delay with the mean node speed for proposed and existing OLSRv2 shown in Figure 4, which can be viewed on the page.12

The Figure 4 describes the relationship between delay with the mean node speed for proposed and existing method. With the increase in node velocity, the trust based routing path is longer which offers the minimum delay compared to existing insecure OLSRv2.

4.3 Throughput

The measure of total size of correct received packets by the destination for each second called as throughput. The analysis of throughput with the number of malicious nodes for proposed and existing OLSRv2 shown in Figure 5.

The Figure 5 describes the relationship between throughput with the number of malicious nodes for

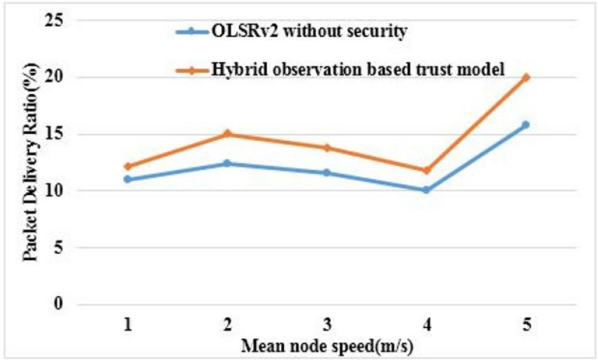

Figure 3. Packet Delivery Ratio vs. Mean node speed.

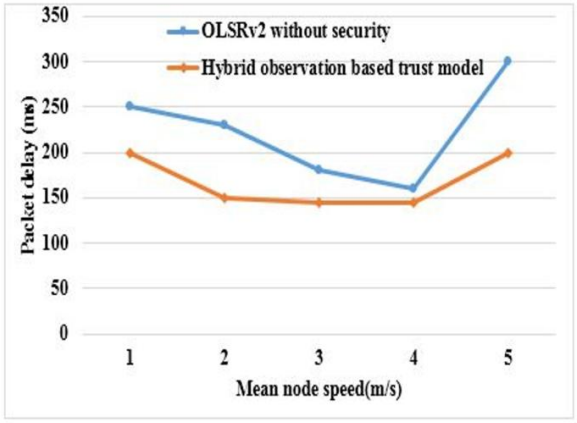

Figure 4. Packet delay vs. Mean node speed.

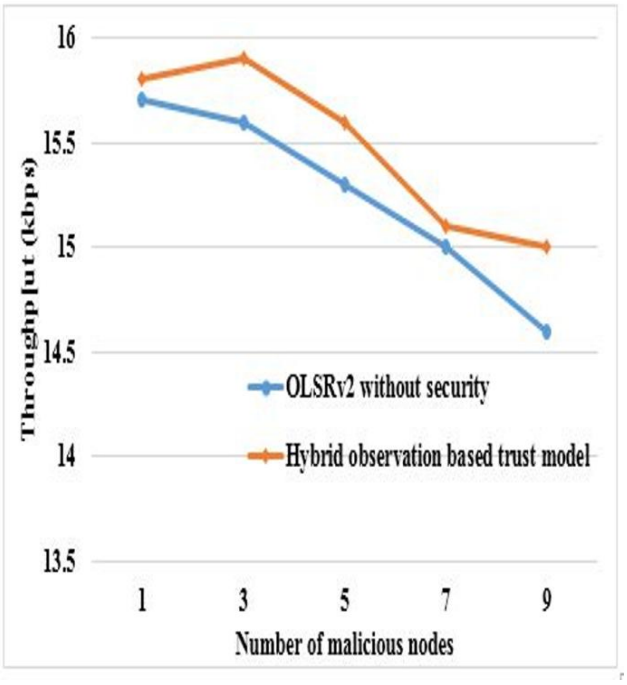

Figure 5. Throughput vs. Malicious nodes.

proposed and existing method. With the increase of malicious nodes, the effective separation of malicious behavior from the faulty behavior by the hybrid observation model provided the high throughput compared to existing insecure OLSRv2.

5. Conclusion

In this paper, the creation of secure environment in MANET using uncertain reasoning methods originates from the artificial intelligence discussed. Direct and indirect observation based trust evaluation performed to show the assurance of security level. The utilization of full probability model in Bayesian interface evaluated the trust from the observer node in direct observation scheme. Alternatively, the neighbor hop information is used in the derivation of trust value in indirect observation scheme. The trust value calculation from the observation schemes governed by Dempster-Shafter Theory (DST), which is another uncertain reasoning. Finally, the Dijkstra's algorithm established the routing process on the basis of shortest path. The comparative analysis of proposed hybrid model with the existing model proved the effectiveness on the parameters of Packet Delivery Ratio (PDR), throughput with less overhead for variation in number of nodes and node speed.

6. References

1. Cho J-H, Swami A, Ing-Ray C. A Survey on Trust Management for Mobile Ad Hoc Networks. Communications Surveys and Tutorials, IEEE. 2011;13(2):562–83.
2. Han G, Jiang J, Shu L, Niu J, Chao H-C. Management and applications of trust in Wireless Sensor Networks: A survey. Journal of Computer and System Sciences. 2014; 80(1):602–17.
3. Govindan K, Mohapatra P. Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey. Communications Surveys and Tutorials, IEEE. 2012; 14(1):279–98.
4. Clausen T, Herberg U. Vulnerability analysis of the optimized link state routing protocol version 2 (OLSRv2). IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), Beijing, China, 2010. p. 628–33.
5. Shengrong B, Yu F-R, Liu X-P, Mason P, Tang H. Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Ad Hoc Networks. IEEE Transactions on Vehicular Technology. 2011; 62(7):1025–36.
6. Bu S, Yu F-R, Liu X-P, Tang H. Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks. IEEE Transactions on Wireless Communications. 2011; 10(9):3064–73.
7. Das A, Islam MM. SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems. IEEE Transactions on Dependable and Secure Computing. 2012; 9(2):261–74.
8. Guan Q, Yu F-R, Shengming J, Leung V-C-M. Joint topology control and authentication design in mobile ad hoc networks with cooperative communications. IEEE Transactions on Vehicular Technology. 2012; 61(6):2674–85.
9. Marchang N, Datta R. Light-weight trust-based routing protocol for mobile ad hoc networks. Information Security, IET. 2012; 6(2):77–83.
10. Subramanian S, Ramachandran B. Trust based scheme for QoS assurance in mobile ad-hoc networks. Networking and Internet Architecture. 2012; 77–84.
11. Persis DJ, Robert TP. Ant Based Multi-objective Routing Optimization in Mobile AD-HOC Network. Indian Journal of Science and Technology. 2015; 8(9):875–88.
12. Zhang R, Zhang Y, Fang Y. AOS: an anonymous overlay system for mobile ad hoc networks. Wireless Networks. 2011; 17(4):843–59.
13. Li W, Joshi A, Finin T. CAST: Context-Aware Security and Trust framework for Mobile Ad-hoc Networks using policies. Distributed and Parallel Databases. 2013; 31(4):353–76.

14. Eissa T, Abdul Razak S, Khokhar R, Samian N. Trust-Based Routing Mechanism in MANET: Design and Implementation. Mobile Networks and Applications. 2013; 18(5):666–77.
15. Adnane A, Bidan C, de Sousa RT Jr. Trust-based security for the OLSR routing protocol. Computer Communications. 2013; 36(10-11):1159–71.
16. Pinyol I, Sabater-Mir J. Computational trust and reputation models for open multi-agent systems: A review. Artificial Intelligence Review. 2013; 40(1):1–25.
17. Gupta N-K, Garg A. Trust and Shortest Path Selection based Routing Protocol for MANET. International Journal of Computer Applications. 2013; 76(12):20–23.
18. Heena Kumar N. Battery power and trust based routing strategy for MANET. International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram. 2014. p. 1559–62.
19. Yanwei W, Yu F-R, Tang H, Minyi H. A mean field game theoretic approach for security enhancements in mobile ad hoc networks. IEEE Transactions on Wireless Communications. 2014; 13(1):1616–27.
20. Teacy W-T-L, Luck M, Rogers A, Jennings N-R. An efficient and versatile approach to trust and reputation using hierarchical Bayesian modelling. Artificial Intelligence. 2012; 193(2):149–85.
21. Yang B,Yamamoto R,Tanaka Y. Dempster-Shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs. 16th International Conference on Advanced Communication Technology (ICACT), Pyeongchang. 2014. p. 223–32.