Received: March 28, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Anomaly-Based Intrusion Detection System with Multi-Dimensional Trust Parameters for Mobile Ad Hoc Network

Sharmasth Vali Yeruru [1]* Tiruchirai Ramanujam Rangaswamy[2]

[1]*B.S.Abdur Rahman Crescent University Chennai-600048, Tamilnadu, India*
* Corresponding author's Email: vali566@gmail.com

Abstract: The distinctive aspect of Mobile Ad Hoc Networks (MANETs), including dynamic network topology, susceptible wireless medium, limited battery power, network overhead are highly vulnerable and remains as major issues in designing Intrusion Detection Systems (IDS). This paper proposes a framework of Anomaly IDS with Subjective logic based Trust (AID-ST) system to discern and eradicate the intruders from the network. AID-ST system incorporates multi-dimensional trust parameters and subjective logic theory to effectively detect and confirm the attack behavior. The system measures indirect trust of a node using subjective logic theory, and IDS estimates trustworthiness of a suspected node by collecting and combining the evidence from various observers. The simulation results depict that the AID-ST attains high performance in terms of detection accuracy, overhead, and energy consumption when compared to existing AIPD AODV.

Keywords: MANET, Anomaly-based intrusion detection system, Network layer attacks, Multi-dimensional trust parameters, Subjective logic based trust.

1. Introduction

The emergence of wireless communication and proliferation of handheld devices is driving a revolutionary change in Mobile ad hoc networks (MANETs). MANET comprises of mobile nodes that operate independently in the open medium without any infrastructure [1, 2]. The nodes in MANET communicate with each other through single or multi-hop. The nodes play the role of a router and compel the nodes to cooperate for the correct operation of the network. The resources are consumed rapidly due to the network activities of nodes. The battery power is one of the major concerns in an open MANET environment. The distributed and open medium of MANET makes it susceptible to a variety of attacks. The reactive and proactive routing protocols are vulnerable to routing attacks as they work on the assumption that all the nodes are cooperative. The malicious nodes use cooperative routing algorithms to launch routing attacks. The widespread routing attacks launched in MANET are the sleep deprivation attack, the black-hole attack, the link withholding attack, the replay attack, the packet dropping attack, the rushing attack, the newcomer attack and Sybil attack. The routing protocols need to deal with node mobility, limitation of battery power, and bandwidth. Due to the MANET characteristics, the conventional centralized monitoring scheme is not feasible in MANETs. All these scenarios motivate researchers to develop an Intrusion Detection System (IDS).

The intrusion exposes the integrity, confidentiality, or resource availability. An IDS is a system developed for detecting such intrusions [3]. Intrusion detection and prevention approaches are the primary solutions to minimize possible intrusions. Developing IDS is overly complex and difficult in MANET compared to fixed networks due to the constraints in accomplishing the requirements of IDS such as the capability to aggregate audit data from the network and detect intrusions with a low rate of false positives. Based on the detection method, the IDS techniques are classified into three categories, named as an

anomaly based, misuse based, and specification based. An anomaly-based IDS technique quantitatively defines the training data of a normal node activity, and it marks the behavior that is deviating from the training data as malicious. Although the anomaly based IDS detects the unknown attacks, it increases the false alarm rate. The misuse based IDS implements a signature based analysis method in which the malicious behavior is detected by comparing the input traffic signature with the known attack signatures. Thus, it limits the IDS to detect the unknown attacks and degrades the network performance. In specification-based IDS, the observed behavior is compared with the correct behaviors of nodes are abstracted as security specifications to detect the malicious behavior. Consequently, the specification-based IDS requires a regular update of specifications, and it is tough in MANET environment. Compared to fixed infrastructure networks, the MANETs are more susceptible to different kinds of security attacks due to lack of a trusted centralized authority. Even though high false alarm rate is a primary concern for developing the anomaly based IDS, it is most suitable to detect the MANET routing attacks. In MANETs, no neighbor can always ascertain that the observed data of a node is normal or anomalous, and something is neglected by existing works which are called as uncertainty. The subjective logic theory is a suitable proposition to model the situations with consideration of uncertainty [4].

This paper proposes a framework of Anomaly IDS with Subjective logic based Trust (AID-ST) system integrating multi-dimensional trust parameters and subjective logic theory that improves the detection performance over malicious network traffic. The multi-dimensional trust factors such as collaboration and behavioural trust represent the node cooperation in routing activities and integrity of transmitted packets respectively. These factors tend the AID-ST to detect both the active and passive attacks. The usage of subjective logic theory reduces the uncertainty with respect to the base rate that represents the expected level of an opinion. To reduce the computational complexity without reducing the accuracy of AID-ST, this work monitors the normal network behaviour and executes the subjective logic, when the node activity differs from the normal behaviour.

1.1 Contribution

The main contributions of the AID-ST system are as follows.

- The main contribution of the AID-ST system is to detect both the active and passive attacks in MANET. The AID-ST comprises multi-dimensional trust parameters to achieve its objectives.
- To minimize the energy consumption and to enhance the routing performance of malicious network traffic, the AID-ST system executes subjective logic theory, only when a malicious activity is detected in the network.
- To train the anomaly IDS, the AID-ST fixes a network characteristic threshold by continuously monitoring the normal activities of nodes for a particular time interval.
- To detect and isolate the malicious nodes from routing activities, the IDS compares the observed data with a network characteristics threshold, and it generates an alarm to collect the recommendations as evidence from neighboring IDS for attack confirmation.
- To confirm the malicious activity by accurately estimating the trustworthiness of a node, the IDS fuses the evidence that is collected from neighboring nodes of a suspected nose using the subjective logic method.

To validate the proof of neighboring nodes and to reduce the uncertainty in evidence collection, the AID-ST utilizes the subjective logic method that exploits a base rate operator to estimate the expectation of an opinion level.

1.2 Paper organization

This paper is organized as follows. Section 2 surveys the works related to the AID-ST system. This section includes the conventional works under the categories of subjective logic based trust estimation and anomaly based IDS techniques. Section 3 describes the system model and Section 4 explains the components of the AID-ST system. It includes training and testing phase of AID-ST, subjective logic based trust estimation, and moreover the intrusion identification. Section 5 illustrates the performance evaluation of AID-ST by varying the number of nodes, and the number of malicious nodes. The performance of AID-ST is measured regarding intrusion detection accuracy, packet delivery ratio, false positive, throughput, delay, and overhead. Section 6 concludes the paper with a few ideas for future work.

2. Literature survey

The characteristics of MANET are vulnerable to several types of attacks. A survey in [5] discusses various types of black hole attack in MANET. An overview of wormhole attack and its types has been surveyed in [6]. The work in [7] analyzes the impact of packet dropping attacks against MANET routing protocols. Several attempts have been made in recent years to identify the intrusion in MANETs. A few IDS techniques measure the trustworthiness of a node to detect misbehavior.

2.1 Subjective logic based trust estimation

Providing quantitative evidence is essential for intrusion detection after self-monitoring on each node in MANETs. The subjective logic is involved in offering quantitative neighbours opinions about the suspicious data of the node. The subjective logic theory is most suitable to collect and to fuse the evidence when the evidence is uncertain. The work in [8] extends the subjective logic to incorporate partial observations when considering the reported classes are unclear. A subjective logic based approach to estimate the trustworthiness of information sources within a specific context, and it overcomes the uncertainty during data fusion [9]. The work in [10] proposes an Opinion Distance based Reputation model to resist selfish behaviours and collusion attacks in MANET. The reputation model evaluates trust between nodes using the subjective logic theory, and it is represented by opinions. The reputation model quickly detects and isolates the malicious nodes. It excludes the malicious recommendations by exploiting the distance of opinion. Moreover, the reputation model is comparatively invulnerable to collusion attacks. A probabilistic asymmetric key pre-distribution in [11] chooses a most reliable and trustful path among the available paths by estimating trust. The subjective logic theory is employed to model trust relationship between nodes and also path conditions.

In emergency situations, the nodes need to communicate and collaborate with each other and evaluating the trustworthiness of nodes play an important role. The work in [12] proposes a trust model based on the subjective logic that represents a belief, disbelief, and uncertainty of the nodes in an uncertain environment. The trust model is adopted in emergency cases that are constructed with MANET. An SLAD framework considers the uncertainty of neighbors to the data of the node [13]. In SLAD, each neighbor provides the quantitative opinion of a node. The subjective logic theory fuses the views of all the neighbors, and it gets the expectation of the opinion. The expectation of opinion demonstrates that the degree of the suspicious data is considered as malicious. To reduce the hazards from malicious nodes, the work in [14] incorporates the trust concept into MANET, and it builds a subjective trust management model with multiple decision factors. Moreover, the subjective logic based trust model improves the detection accuracy over high malicious network traffic.

2.2 Anomaly based IDS techniques

The work in [15] comprehensively surveys the anomaly based intrusion detection techniques with advantages, and disadvantages. Further, it evaluates the performance of anomaly-based IDSs. A cooperative, distributed intrusion detection architecture for MANETs has been proposed in [16]. The main objective of the cooperative and distributed IDS is to detect the attacks by taking right decision based on the data that collects from various nodes. The distributed and cooperative approach possibly minimizes detection latency and bandwidth consumption. The work in [17] Reviews the most well-known anomaly-based intrusion detection techniques.

An anomaly-based intrusion detection protocol (AIDP) detects and isolates the sleep deprivation attack using a combination of the chi-square goodness of fit test and control charts [18]. An approach in [19] models the normal behavior of the network using three feature vectors and identifies the black hole attack with the help of the ABID discrimination module. The work in [20] provides a comprehensive survey of anomaly detection techniques for MANETs. An anomaly-based IDS for gray hole attack detection has been proposed in [21]. The anomaly IDS exploits a simple threshold to detect the gray hole attacks in the networks. It lacks to consider the network conditions into account, and thus, it reduces the attack detection accuracy. An anomaly-based intrusion detection system for packet dropping attack has been proposed in [22].

Most of the existing anomaly based IDS schemes attain a high number of false positives due to lack of considering multiple trust parameters into account. Therefore, it is crucial to introduce a multi-dimensional trust based IDS system to detect efficiently and mitigate the effect of intruders over MANET.

3. System model

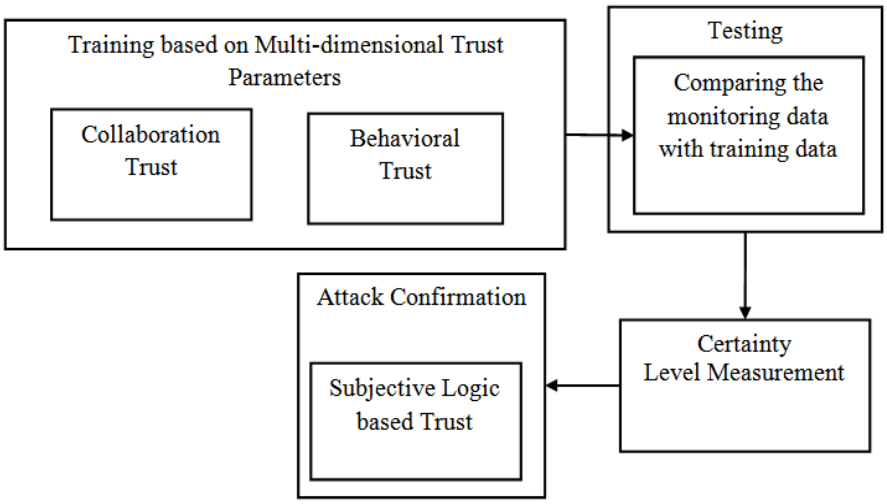

Figure.1 Block diagram of AID-ST system

Network size is represented as $X \times Y$. The network is represented as a communication graph G (N, E). The network G contains the number of nodes that are represented as N. The communication range of a node is represented as R and R=250 for simulation. The set E contains all directional links between node A and B, where A, $B \oplus N$. In AID-ST, the anomaly based IDS exploits multi-dimensional trust factors to detect the attack behavior. The AID-ST fixes Network characteristics (NC_{th}) to train the IDS. In the testing phase, the AID-ST measures a trustworthiness of a node regarding certainty level (CL) and detects the malicious behavior by comparing the CL and NC_{th}. The misbehaving probability is denoted as P_m that is calculated based on subjective logic theory. The subjective logic theory exploits a dynamic base rate (a) that calculates the expectation of opinion level. The base rate is dynamically varied according to the number of positive evidence (p), collected in the current time interval (i).

4. AID-ST system overview

The main objective of the AID - ST system is to detect and mitigate the effect of active and passive attacks on the network by designing an anomaly based IDS model. To detect and confirm the malicious behavior in the network, the AID-ST architecture consists of three major phases such as training, testing, and subjective logic based trust measurement. Figure 1 depicts the block diagram of AID-ST. In AID-ST, each node monitors the network continuously and collects the data for a particular time interval to train the anomaly IDS. The AID-ST trains the anomaly IDS by incorporating multi-dimensional trust factors that are collaboration trust and behavioral trust. The multi-dimensional trust factors assist to categorize various kinds of misbehavior occurred in different contexts over MANETs. In testing, the anomaly IDS compares the current monitoring data with the training data to measure the certainty level of the attacker. If the certainty level is high, the AID-ST isolates the malicious node from routing activities. Otherwise, the AID-ST requires measuring the indirect trust value of a node that has low certainty level based on SLT to confirm the attack behavior.
The IDS evaluates the trustworthiness by collecting evidence from the neighboring IDSs of the suspected node and combines the evidence using subjective logic. The base rate of SLT reduces the uncertainty in deciding trustworthiness of a node by estimating an expectation of opinion. Moreover, the IDS accurately identifies the attacker and enhances the network performance.

4.1 Training phase of AID-ST

In general, disparate categories of malicious behaviours may occur in a different context over MANETs. Most of the conventional trust mechanisms only take into account the packet dropping features in measuring the trustworthiness of a node. Hence, such mechanisms detect all type of node misbehavior on a uniform scale by estimating trustworthiness. To effectively categorize different types of malicious behaviors, the AID-ST takes into account different features of malicious behaviors in trust evaluation. In AID-ST, each node equipped with an IDS to measure its behavior and its neighboring nodes behavior. In training phase of AID-ST, each node fixes a Normal Characteristics (NC) threshold by monitoring the normal network activities for a certain period.

$$NC_{th} = W1 \times T_{c(th)} + W2 \times T_{b(th)} \quad (1)$$

In equation (1), the NC_{th}, $T_{c(th)}$, and $T_{b(th)}$ refer the threshold of *NC*, collaboration trust, and behavioral trust respectively. The terms *W1* and *W2* are weighting factors. The summation value of the weighting factors is equal to one. In the training phase, the nodes continuously monitor and record data about the collaboration, and behavioral trust parameters for fixed time intervals and create a statistical model that describes the normal behavior of a node. Besides, the initial training data reflect the normal behavior of the nodes in the network and the expected level of network performance.

4.2 Testing phase of AID-ST

It is crucial that an IDS not only determines a malicious behavior, whereas it also detects the attack type and the attacker whenever possible. The AID-ST measures multi-dimensional trust parameters to detect the malicious behaviors and also specific attack types. The basic idea is to determine the detailed attack information from a set of identification rules, which are pre-computed for known attacks. In the testing phase, each IDS monitors the behavior of nodes and compares the monitored data with the training data to analyze the deviations. The IDS evaluates Certainty Level of a node n (CL_n) based on multi-dimensional trust factors such as collaboration trust (T_c), and behavioral trust (T_b). The AID-ST measures trust of a node n using equation (2).

$$CL_n = W1 \times T_c + W2 \times T_b \quad (2)$$

T_c Estimation: The collaboration trust is measured based on node cooperation in network activities such as control and data packet forwarding. T_c is evaluated by identifying the amount of abnormal behavior including data and control packet dropping. The IDS estimates T_c using equation (3).

$$T_c = \{(\sum_{i=1}^{M} CPF_i)/m) + (\sum_{j=1}^{n} DPF_j)/n)\} / 2 \quad (3)$$

Where, the terms CPF_i and DPF_i represent control packet forwarding and data packet forwarding respectively. The term m and n refer the total number of control and data packets between two adjacent neighbors.

T_b Estimation: During testing, the IDS obtains the behavioral trust of a node by measuring modified packet count (N_d), delayed delivered packet count (N_q), and quickly delivered packet count (N_m). The IDS estimates T_b using equation (4).

$$T_b = \left\{\left(\frac{N_d}{n}\right) + \left(\frac{N_q}{n}\right) + \left(\frac{N_m}{n}\right)\right\} / 2 \quad (4)$$

In equation (4), the term *n* refers the total number of packets that are forwarded in a particular time interval. The AID-ST estimates the N_d based on TTL value of the forwarding packet. If the TTL value is greater or very less than the actual TTL, the AID-ST updates the N_d as one. Otherwise, the N_d value is zero. Likewise, the AID-ST calculates the number of delayed and quickly delivered packets. The nodes measure modified packet count by overhearing the communication of its neighboring nodes. The AID-ST applies the equations (3) and (4) in equation (2) to evaluate the trustworthiness of a node n. Moreover, the AID-ST compares the T_n value with the NC_{th} to decide the certainty level of a node n. If the CL_n value is greater than the NC_{th}, the IDS conclude the node n is a good node. On contrast, the T_n value is very lesser than the NC_{th}; the IDS generates an intrusion alarm to collect and combine the evidence from the neighboring nodes of a suspected node to confirm the malicious behavior.

4.2.1. Subjective logic based trust (SLT) estimation

Each node keeps a trust table that associates a trust value to each of its neighboring nodes. Every node obtains the table on routing observation. The trustworthiness of a neighbor node is not distributed globally while it is kept locally. The neighboring nodes that receive an intrusion alarm share their observations about the suspected node to the corresponding IDS. The IDS exploits subjective logic that enables mobile nodes to represent explicitly and manage the uncertainty when the collected evidence are distinctive. The important parameter of subjective logic is the base rate, as the base rate dynamically evaluates an expectation of opinion according to the number of positive evidence. The expectation of opinion reduces the uncertainty in evaluating the trustworthiness of a suspected node.

Consider node (*u*) and (*v*) are neighbors of suspected node (*s*). The IDS of suspected node collects evidence from node u and v to evaluate the trustworthiness. The evidence (ω) consists of three dimensions such as a belief (*b*), disbelief (*d*), and uncertainty (*u*). The terms *b* and *d* represent the benign and malicious behavior of s respectively. The

term u is the ignorance or level of confidence in node's knowledge about suspected node. The ω_s^u and ω_s^v represent the evidence that is collected from node *u* and *v* respectively. The IDS examines whether the information in evidence is observed in the same time interval or not. If the evidence is observed in a different time interval and $U_s^u \neq 0$ V $u_s^v \neq 0$, the IDS fuses the evidence as follows equation (5) and equation (6).

$$w_s^u \oplus w_s^v = \begin{cases} b_s^u \oplus b_s^v = b_s^u\, u_s^v + b_s^v\, u_s^u / k \\ d_s^u \oplus d_s^v = d_s^u\, u_s^v + d_s^v\, u_s^u / k \\ u_s^u \oplus u_s^v = u_s^u\, u_s^v / k \end{cases} \quad (5)$$

Where,

$$k = u_s^u + u_s^v - u_s^u\, u_s^v \quad (6)$$

If nodes *u* and *v* observe the behaviour of a suspected node in the same time interval and $U_s^u \neq 0$ Λ $u_s^v \neq 0$, the AID-ST fuses the evidence using Eq. (7).

$$w_s^u \oplus w_s^v = \begin{cases} b_s^u \oplus b_s^v = b_s^u\, u_s^v + b_s^v\, u_s^u / k \\ d_s^u \oplus d_s^v = d_s^u\, u_s^v + d_s^v\, u_s^u / k \\ u_s^u \oplus u_s^v = 2\, u_s^u\, u_s^v / k \end{cases} \quad (7)$$

Where,

$$k = u_s^u + u_s^v \quad (8)$$

The IDS of suspected node has received a huge amount of evidence from various independent observers. The IDS evaluates a total trust value, *T* of suspected node using the fused evidence and base rate operator. The *T* value is estimated using equation (9).

$$T = \sum_{i=1}^{N} b_s^i \times a(x_i) \quad (9)$$

Where b_s^i is the belief value of i^{th} fusion of observed information. The term *a(x)* represents the base rate that is evaluated using the number of positive evidence collected at a particular time. Initially, the base rate value is one, and it varies according to the number of positive evidence. Moreover, the AID-ST takes weighted average to the *CL* and *T* of a suspected node for estimating final trust.

4.3 Intrusion identification

In AID-ST system, the IDS fixes an NC_{th} by observing the routing functions of nodes for a particular time interval. The AID-ST compares the CL_n value with the NC_{th} that is estimated using network characteristics, and it generates an intrusion alarm to estimate the indirect trust when suspicious activity is detected. The IDS evaluates the trustworthiness of a suspected node using the SLT model. The IDS decides whether a suspected node is legitimate or malicious based on the final trust value that is estimated using *CL* and *T*. The final trust value is high when suspected node involves extensive interactions with its neighbors. If the final trust value is high, the AID-ST system concludes that the suspected node is benign, and the generated alarm is false. On the contrary, the final trust value of *s* is low, when s involves several harmful interactions. Consequently, the AID-ST system marks the suspected node as malicious. Moreover, the AID-ST system selects the highly trusted nodes as routers and enhances the routing efficiency.

5. Performance evaluation

The performance of the AID-ST system is analyzed through Network Simulator (NS-2), and it is compared with the existing AIPD [22]. The simulation is performed on a random topology of 100 nodes with the speed of 25m/s over a network area of 1000m x 1000m. The initial energy of a node is 10J, and the communication range is 250m. This work exploits a Dynamic Source Routing (DSR) protocol for packet forwarding. The AID-ST exploits Constant Bit Rate (CBR) and Transport Control Protocol (TCP) in the application layer and the transport layer respectively. A packet size is 1024 bytes, and the packet transmission interval is four milliseconds. The Random Way Point (RWP) mobility model is used for node mobility. In RWP, the mobile nodes move in a random direction and pause for 60 seconds. The total simulation time is 100 seconds.

5.1 Experimental results

The efficacy of the proposed AID-ST system is evaluated using the performance metrics such as Intrusion Detection Accuracy, Packet Delivery Ratio, Throughput, Energy level, Routing Overhead, and Delay.

Intrusion Detection Accuracy: It is the percentage of the number of identified attackers to the total number of attackers.

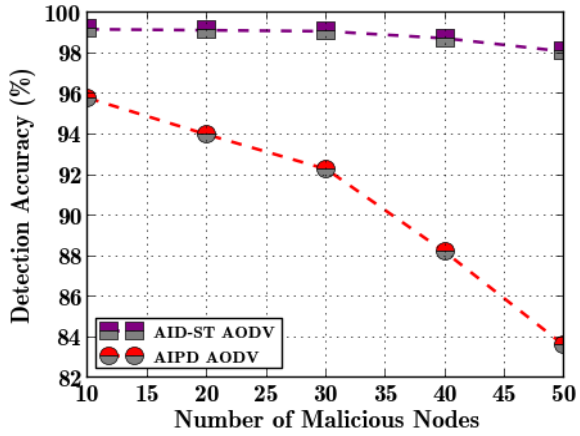

Figure.2 Number of malicious nodes Vs detection accuracy

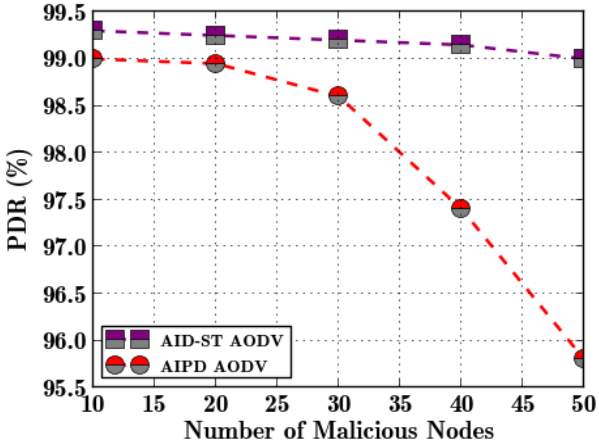

Figure.3 Number of malicious nodes Vs PDR

Packet Delivery Ratio (PDR): It is the percentage of successful packet delivery of the total number of generated packets.

False Positive: It is the percentage of good nodes that are falsely identified as attackers.

Throughput: It is the rate of successful data delivery.

Overhead: It is the number of additional packets generated to select the most trustworthy routers.

Delay: It is the amount of time taken by a packet to reach the destination from the source.

5.1.1. Impact of number of malicious nodes

Figure 2 shows the detection accuracy results of both the AID-ST AODV and the AIPD AODV by varying the number of malicious nodes. From Fig. 2, the AID-ST AODV maintains its detection accuracy even the number of malicious nodes are high.

The AID-ST AODV detects the suspected behavior based on collaboration and behavioral trust values of nodes. Further, the AID-ST AODV protocol confirms the attack behavior by collecting evidence from neighboring nodes, and it takes a decision based on subjective logic evidence fusion. The dynamic base rate evaluates an expectation of opinion in each interval, and thus, it maintains the decision-making accuracy when the number of malicious nodes is increased. For instance, the AID-ST AODV attains 99.2% and 98.1% of detection accuracy for the number of malicious nodes of 10 and 50 respectively. The AIPD AODV protocol detects the malicious behavior based on a simple threshold measurement, and it does not consider the trustworthiness of a node in attack detection. As a result, the detection accuracy decreases. The AID-ST AODV system improves the detection accuracy by 14.5% more than that of AIPD AODV under the high malicious scenario.

Figure 3 depicts the PDR results of AID-ST AODV and AIPD AODV protocols by varying the number of malicious nodes. Both the AIPD AODV and AID-ST AODV protocols decline the PDR when increasing the number of malicious nodes from low to high.

For instance, the AID-ST AODV protocol decreases the PDR by 0.3%, when varying the malicious nodes from 10 to 50. Even though the halves of the network nodes are malicious; the AID-ST AODV protocol maintains its superior PDR. The reason is that the base rate operator in subjective logic trust measurement assists AID-ST AODV to detect the malicious nodes accurately under the high malicious scenario that contains untrustworthy evidence. The base rate increases the trust decision accuracy by estimating an expectation of opinion according to the number of positive evidence when the number of attackers is high. Besides, the performance of AID-ST AODV is higher than the AIPD AODV. Figure 3 illustrates that the AID-ST AODV escalates the PDR by 3.2% when compared to the existing AIPD AODV when half of the nodes are malicious in the network.

Figure 4 shows the false positive results of both the AID-ST AODV and the AIPD AODV protocols by varying the number of malicious nodes from low to high. Figure 4 clearly shows that the AID-ST AODV attains minimum false positives when compared to existing AIPD AODV protocol. The reason behind this that the AID-ST AODV detects the malicious behavior based on collaboration and behavioral based trust measurement. Further, it confirms the malicious behavior based on subjective logic trust measurement.

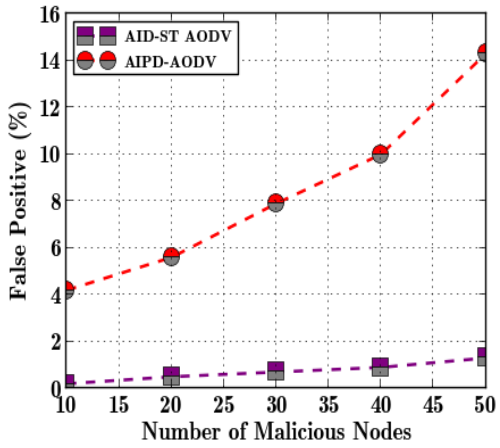

Figure.4 Number of malicious nodes Vs false positive

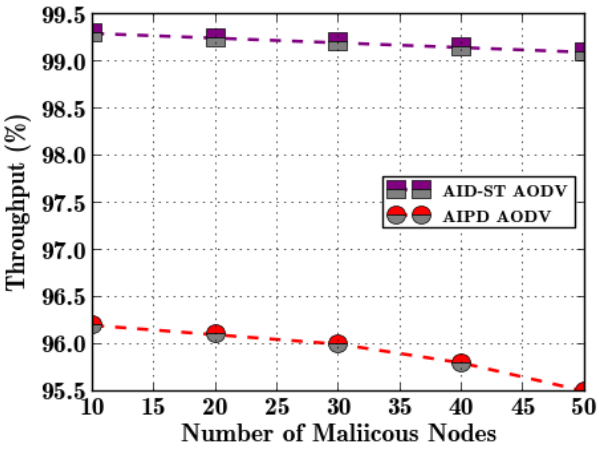

Figure.5 Number of malicious nodes Vs throughput

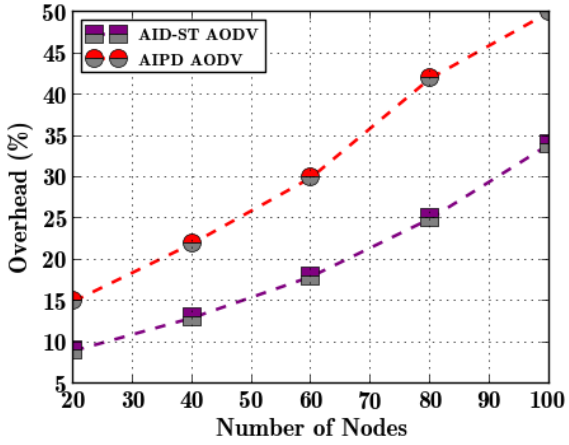

Figure.6 Number of nodes Vs overhead

The AIPD AODV protocol lacks to take into account the multi-dimensional trust values in attack detection. Moreover, the AID-ST achieves higher detection accuracy than existing AIPD AODV and, thus it reduces the false positive rate considerably. For instance, the AID-ST AODV and AIPD AODV attain 1.3% and 14.3% of false positives respectively, when the number of malicious nodes is 50.

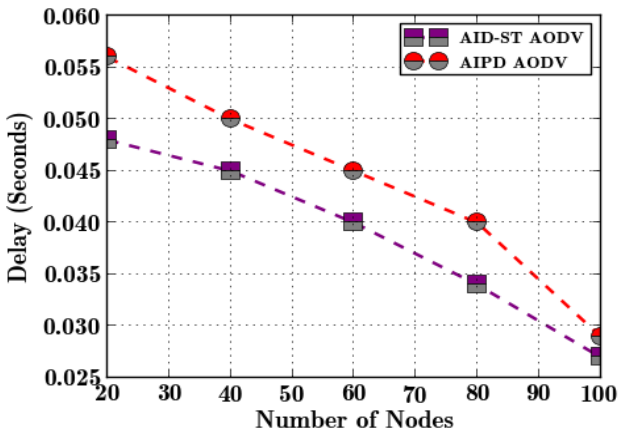

Figure.7 Number of nodes Vs delay

Figure 5 shows the throughput results of both the AID-ST AODV and the AIPD AODV protocol by varying the number of malicious nodes from low to high. The AID-ST AODV protocol selects trustworthy nodes as routers, and it maintains the throughput when increasing the number of malicious nodes from 10 to 50. Unlike AIPD AODV, the AID-ST AODV protocol detects most of the attacks in route discovery phase, as it considers multi-dimensional factors in trust evaluation. Consequently, the AID-ST AODV attains higher throughput than AIPD AODV. For instance, the AID-ST AODV increases the throughput by 3.6% more than that of AIPD AODV under the high malicious scenario.

5.1.2. Impact of number of nodes

Figure 6 shows the results of the overhead of AID-ST AODV and AIPD AODV protocols by varying the number of nodes from low to high. The overhead of both the AID-ST AODV and AIPD AODV protocols increase when the number of nodes are increased from low to high. For instance, AID-ST AODV increases the overhead by 25%, when varying the number of nodes from 20 to 100. Although AID-ST AODV exploits control packets to collect evidence from various observers, the overhead of AID-ST AODV is acceptable, as only the indirect trust is evaluated on a suspected node.
The AID-ST AODV varies the trust threshold dynamically based on the network conditions. Thus, it increases the attack detection accuracy. Unlike AID-ST AODV, the AIPD AODV fixes threshold using multi-dimensional trust factors, and it increases the false positives. Moreover, the AID-ST AODV reduces the overhead, when compared to AIPD AODV. In Fig. 6, the AID-ST AODV and AIPD AODV attain 34% and 50% of overhead respectively, when the number of nodes is 100.

From Fig.7, both the AID-ST AODV and AIPD AODV protocols decrease the delay, when increasing the number of nodes from low to high. The reason behind this is due to the presence of a huge number of nodes in the network that increases the connectivity, and the packets get rapidly delivered to the destination. For instance, the AID-ST AODV attains delay of 0.048 seconds and 0.027 seconds for 20 and 100 of node density respectively. Although, when compared to AIPD AODV, the AID-ST AODV achieves minimum delay, as it considers the trustworthiness of a node in router selection. From Fig. 7, the AID-ST AODV reduces the delay by 14.28% less than that of AIPD AODV for 20 nodes.

6. Conclusion

This paper concentrates on the intrusion detection problem in the MANET and proposes an AID-ST that exploits an anomaly based IDS and subjective logic based trust components to discover and mitigate the effects of attackers. The framework adds a field in MANET routing protocol to obtain independent observations. The threshold measurement depends on the collaboration and behavior trust of nodes. In IDS an intrusion alert based on the threshold variation and confirms the attack behavior by estimating indirect trust of nodes. The AID-ST evaluates the indirect trust of a node using subjective logic based evidence fusion. Thus, the AID-ST system reduces uncertainty by exploiting the advantage of the base rate operator. The simulation results demonstrate that the AID-ST attains higher performance in terms of detection accuracy, PDR, delay, and overhead, compared to existing AIPD. In the future work, to further improve the accuracy of collaborative trust measurement in AID-ST, plans to enable the node to include the contextual information such as mobility and energy. This work completely ignores the effect of contextual factors and improves the attack detection accuracy.

References

[1] I. Chlamtac, M. Conti, and J.J-N. Liu “Mobile ad hoc networking: imperatives and challenges”, *Ad hoc Networks, ELSEVIER,* Vol.1, No.1, pp.13-64, 2003.

[2] C.M. Cordeiro and D.P. Agrawal “Mobile ad hoc networking”, *Centre for Distributed and Mobile Computing,* pp.1-63, 2002.

[3] Y. Zhang, W. Lee, and Y. Huang, “Intrusion detection techniques for mobile wireless networks”, *Mobile Networks and Applications,* Vol. 9, No.5, pp. 545-556, 2003.

[4] B. Venkat, V. Vijay, and T. Uday, “Subjective Logic Based Trust Model for Mobile Ad hoc Networks”, In: *Proc. of 4th International Conf. On Security and Privacy in communication networks, SecureComm ’08,* Istanbul, Turkey, 2008.

[5] F. Tseng, L. Chou, and H. Chao, “A survey of black hole attacks in wireless mobile ad hoc networks”, *Human-centric Computing and Information Sciences, Springer,* Vol. 1, No. 4, pp. 1-16, 2011.

[6] S. Akansha and D. Rajni , “Wormhole Attack in Mobile Ad-hoc Network: A Survey”, *International Journal of Security and Its Applications,* Vol. 9, No. 7, pp. 293-298, 2015.

[7] B. Venkatesan and V. Vijay, “Packet drop attack: A serious threat to operational mobile ad hoc networks”, In: *Proc. of International Conf. On Networks and Communication Systems,* pp. 89-95, 2005.

[8] L.M. Kaplan, M. Lance, S. Chakraborty, and C. Bisdikian, “Subjective logic with uncertain partial observations”, In: *Proc. of IEEE 15th International Conf. On Information Fusion (FUSION),* pp. 565-572, 2012.

[9] M. Sensoy, J. Z. Pan, A. Fokoue, M. Srivatsa, and F. Meneguzzi, “Using subjective logic to handle uncertainty and conflicts”, In: *Proc. of IEEE 11thInternational Conf. On Trust Security and Privacy in Computing and Communications (TrustCom),* pp. 1323-1326, 2012.

[10] X. Gu, P. Lin, S. Shi, “A Novel Reputation Model Based on Subjective Logic for Mobile Ad Hoc Networks”, In: *Zhang W. (eds) Advanced Technology in Teaching. Advances in Intelligent and Soft Computing*, vol 163. Springer, Berlin, Heidelberg, Vol.163, 2012.

[11] M. Ahmadi, M. Gharib, and F. Ghassemi, “Probabilistic Key Pre-distribution for Heterogeneous Mobile Ad hoc Networks Using Subjective Logic”, In: *Proc. of IEEE 29th International Conf. On Advanced Information Networking and Applications,* pp. 185-192, 2015.

[12] A.A. Bakar, R. Ismail, A.R. Ahmad, and J. A. Manan, “Subjective Trust Model for Mobile Ad-Hoc Network in Emergency Environment”, *IEEE Symposium on Wireless Technology and Applications (ISWTA),* pp. 297-302, 2012.

[13] J. Yuan, H. Zhou, and H. Chen, “Subjective Logic-Based Anomaly Detection Framework in Wireless Sensor Networks”, *International*

Journal of Distributed Sensor Networks, Vol. 8, pp. 1-13, 2012.

[14] H. Xia, Z. Jia, L. Ju, X. Li, and Y. Zhu, "A Subjective Trust Management Model with Multiple Decision Factors for MANET based on AHP and Fuzzy Logic Rules", In: *Proc. of International Conf. On Green Computing and Communications,* pp. 124-130, 2011.

[15] D. Kheyri and M. Karami, "A Comprehensive Survey on Anomaly-Based Intrusion Detection in MANET", *Computer and Information science,* Vol. 5, No. 4, pp. 132-139, 2012.

[16] D. Sterne, P. Balasubrmanyam, D. Carman, B.Wilson, R. Talpade, C.Ko, R.Balupari, C-Y. Tseng, T. Bowen, K. Levitt, and J.Rowe, "A General Cooperative Intrusion Detection Architecture for MANETs", *Third IEEE International Workshop on Information Assurance,* pp. 57-70, 2005.

[17] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges", *Computers and Security*, Vol. 28, No. 1-2, pp: 18-28, 2009.

[18] A. Nadeem and M. Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service Attacks in Manets", In: *Proc. of ACM International Conf. On Wireless Communication and Mobile Computing Conf. (IWCMC 09*), pp.926-930, 2009.

[19] S. Kurosawa and A. Jamalipour, "Detecting Blackhole Attack on AODV based Mobile Ad Hoc Networks by Dynamic Learning Method", *International Journal of Network Security,*Vol.5, No.3, pp 338-345, 2007.

[20] C. Panos, C. Xenakis, and I. Stavrakakis, "An Evaluation of Anomaly-Based Intrusion Detection Engines for Mobile Ad Hoc Networks", In: *Proc. of International Conf. On Trust, Privacy and Security in Digital Business Springer Berlin Heidelberg, Vol. 6863,* pp. 150-160, 2011.

[21] S. Jain, and S.K. Raghuwanshi, "Behavioural and node performance based Grayhole attack Detection and Amputation in AODV protocol", In: *Proc. of IEEE International Conf. on Advances in Engineering and Technology Research (ICAETR),* pp. 1-5, 2014.

[22] S. Uyyala, and D. Naik, "Anomaly based intrusion detection of packet dropping attacks in mobile ad-hoc networks", In: *Proc. of IEEE International Conf. on Control, Instrumentation, Communication and Computational Technologies (ICCICCT),* pp. 1137-1140, 2014.