AN EFFICIENT CROSS-LAYER BASED INTRUSION DETECTION SYSTEM FOR MOBILE AD HOC NETWORKS

[1]Y.SHARMASTH VALI, [2]T.R.RANGASWAMY

[1]Assistant Professor, Department of CSE, Dhanalakshmi College of Engineering, Chennai, India.
[2]Professor, Department of E&IE, B.S.Abdur Rahman University, Chennai, India.
E-mail: [1]vali566@gmail.com,[2]ramy49@bsauniv.ac.in

ABSTRACT

Recently, the widespread availability of wireless communications has led to the growth and significance of wireless Mobile Ad hoc Networks (MANETs). Among the routing layer attacks, packet dropping is one of the most disruptive threats in MANETs. Thus, the malicious nodes can camouflage under the background of harsh channel conditions and reduces the detection accuracy of conventional secure routing protocols. In such circumstances, observing the packet loss rate is not adequate to accurately identify the exact cause of a packet loss. This paper proposes a Cross-layer based distributed and cooperative Intrusion Detection System (IDS) with Dempster-Shafer evidence theory (CID) system to accurately discern and eradicate the intruders using cross layer information. The CID system includes local detection engine and IDS. A local detection engine continuously monitors the network activity and differentiates the packet loss due to harsh channel conditions from the malicious one using the features of physical, MAC, and network layer. When the local detection engine detects malicious activity, it turns on IDS in a node. The IDS utilizes the Dempster-Shafer (DS) evidence theory to collect evidence only from trustworthy nodes and provides a mathematical way to merge the evidence with direct trust value in confirming the malicious activities. Eventually, the proposed CID system is extended with the AODV routing protocol, and evaluated under malicious network traffic. The simulation results show that the CID system outperforms the existing EAACK in terms of attack detection accuracy, and network lifetime.

Keywords: *MANET, IDS, Packet Dropping Attacks, Cross-Layer, Trust Management, DS Theory*

1. INTRODUCTION

A Mobile ad hoc network (MANET) is a multi-hop wireless network composed of a set of self-configurable mobile nodes that are geographically distributed in a given area and without a centralized administration [1] [2]. In a MANET, the mobile nodes cooperate in relaying/routing traffic and the MANET promises to be the operational base for several applications. However, the security issues are paramount in MANET due to the unreliable communication medium. The malicious node exploits the cooperative nature of MANETs to launch several types of routing attacks. The packet dropping is the most significant security attack in MANET. Once the packet dropping attacker is included in the routing path, it starts to drop the packets maliciously and disrupts the traffic delivery persistently. For instance, in military surveillance, the intruder node may drop the packets with aiming to disrupt the military functionalities. Hence, it is crucial to identify the dropping attacker at the right time to save human lives.

With the aim of detecting the packet dropping attack, several conventional Intrusion Detection System (IDS) schemes measure the trust value through observing the packet loss rate and collect evidence from neighboring nodes. As there is a conflict in collecting evidence, the Dempster-Shafer (DS) theory is a useful technique to ratify the effect of conflict in detection accuracy.

In a MANET, the harsh channel conditions, e.g., interference, link errors due to mobility causes packet dropping in the network. The malicious nodes observe the network knowledge, and it can camouflage its malicious behavior under the background of harsh channel conditions by dropping a few packets. Hence, observing the packet loss rate is not sufficient to precisely identify the packet loss happened due to malicious activities. Clearly, deciding whether a packet loss is intentional or unintentional is a challenging problem in MANET. To distinguish the packet loss due to either network conditions or malicious activities, the existing techniques include the information extracted from multiple layers such as network, MAC and physical in the design of the IDS. These schemes keep the IDS in always on strategy, and they are relatively expensive on MANET because of their high energy consumption, overhead and computational capacity. This paper proposes a Cross-layer based distributed and cooperative IDS with Dempster-Shafer evidence theory (CID) system that exploits cross layer information to accurately detect the malicious activities without consuming a huge amount of energy. The CID effectively differentiates the packet loss due to harsh channel conditions from malicious activities using the features of physical, MAC, and network layer in building the IDS with a considerable amount of energy consumption. In brief, the contribution of the research work is summarized below:

- The CID aims to detect the packet dropping attacks with less energy consumption and to enhance the routing performance over malicious network traffic. The CID adopts two main elements, the local detection engine, and IDS.
- To differentiate the packet loss happened due to harsh channel conditions from malicious actions, a local detection engine employs the features of physical, MAC, and network layer in the packet loss observation.
- To reduce the energy consumption and to improve the routing performance of malicious network traffic,the CID system only turns on the IDS, when the local detection engine detects malicious activity instead of using the IDS in always on strategy.
- To validate the evidence of neighboring nodes and to reduce the false positive rate, the CID utilizes the DS evidence theory and utilizes the most trustworthy evidence in trust evaluation.

This paper organizes as follows. Section 2 discusses the related works to intrusion detection over MANETs. Section 3 describes the system model and explicates the proposed CID system. Section 4 describes the CID. Section 5 illustrates the performance evaluation of CID and section 6 concludes the paper.

2. RELATED WORKS

The DS theory utilized in a distributed intrusion detection system that reflects the uncertainty [4]. This paper accumulates and combines evidence from unreliable observers to determine the intruders. Using a Bayesian approach, it calculates trustworthiness for a single node. The trustworthiness is calculated based on a hypothesis and evidence that is collected from unreliable observers. The Dempster combination rule combines the independent data observed by different nodes. However, the Dempster Shafer theory provides inaccurate trust measurement, when most of the observer nodes are unreliable. A Collaborative Framework for Intrusion Detection Networks (CIDNs) is proposed in [5], that uses a Bayesian theorem for a feedback aggregation scheme for each peer in CIDN. This work connects IDS into the social network. It uses a beta distribution to model the false positive (FP) and true positive (TP) of each IDS. Although, the CIDN system increases the false alarm due to uncertain probability values. The CIDN [6] mechanism provides incentives To encourage the legitimate nodes. The Bayesian scheme reduces the cost of risks of false positives. However, the overhead and power consumption is high in CIDN.

The paper [7] proposes a robust Bayesian trust management model to estimate the level of trustworthiness of participating IDSs due to their mutual experience. In addition, this work adopts the Dirichlet family of the probability density functions to the trust management for evaluating the future action of an IDS based on the history of an IDS. This work determines the intruders effectively**.** The intrusion detection schemes in [8] detect packet dropping attacks and [9] detects the selfish nodes. The work in [10] detects a flooding attack. The work [11] presents a clustered detection technique that periodically elects a monitoring node named as a cluster head. The monitor node is responsible for monitoring the cluster and detecting both local and global intrusions. It abstracts the actual node's behavior on the on-demand routing protocol specification and develops a finite state machine (FSM). The monitor node observes the behavior of each node and detects an attack if any of the node's behavior is not confirmed through the FSM. A cooperative intrusion detection system [12] [13] detect packet dropping attacks using a hierarchical architecture.

The ARAN is a end-to-end authenticated routing scheme that protects the network from malicious nodes [14]. ARAN detects the malicious nodes that cause a denial of service, route redirection, tunneling and routing loops using the certification process. However, the ARAN increases the overhead due to exploiting cryptographic certificates among network entities. The SEAD is a secure routing protocol designed for proactive routing protocol that defends against routing packet modification, advertising, false routing packets, wormhole attacks, and replay attacks using one-way hash function [15]. The work in [16] suggested a specification and synthesis for modeling and analyzing MANET routing protocols. It extracts the specifications from the traffic flow and exploits this specification to detect the intrusions. The specification based approach lacks to assure completeness and consistency in developing the specification. The anomaly detection approach devices a behavior that nodes can use to decide the trustworthiness of other nodes [17], and it checks their technique with an anomalous payload detector. The training phase examines the payload, and it collects payload from different nodes to generate profiles that are compared using a similarity matrix. Moreover, exchanging models between the nodes introduces additional communication and processing overhead.

Intrusion detection for MANETs in [18] is based on the game-theoretic framework. It models a two player Bayesian game that considers the intruder and the detector. It employs Bayesian hybrid detection methods that observe the network in two different ways, such as lightweight and heavyweight systems. The work in [19] proposes an anomaly detection using Markov chain classifiers. The anomaly detection algorithm involves two steps. The first step constructs a Markov chain table and the second step constructs a classifier based on a Markov model. An anomaly-based intrusion detection protocol (AIDP) identifies and eliminates the intruder that causes sleep deprivation attack using a combination of the chi-square goodness of fit test and control charts [20]. An approach in [21] models the proper behavior of the network using three feature vectors and identifies the black hole attack using ABID discrimination module. An intrusion detection engine for mobile ad hoc network uses a neural network and watermarking techniques [22]. A TWOACK scheme has been proposed in [23]. The TWOACK scheme solves the drawback of watchdogs such as a receiver collision and limited transmission power. The TWOACK scheme determines the misbehaving link by receiving ACK. The ACK is received to each data packet, which transmits over every three succeeding nodes along the routing path. Each node sends an ACK to the node that is two-hop apart from it. Likewise, the TWOACK scheme resolves limited transmitted power and receiver collision. However, the network overhead increases when receiving ACK from a node that is two-hop apart from the sender. The overhead and energy consumption is high in TWOACK.

The existing schemes are lacking in accurately deviate the packet loss happened due to network conditions or malicious activities. In addition, most of the conventional work keeps the IDS at always on strategy and thus, leads to high energy consumption in the network. The proposed CID is an energy efficient system that utilizes cross layer information to deviate the packet loss happened due to the malicious activities.

3. CID SYSTEM OVERVIEW

The packet dropping attack is the most disruptive threat in MANETs. Instead of forwarding the received data or the routing messages, the attackers maliciously drop the packets and disrupt the normal operation of the network. Observing the network layer activities is not adequate to precisely identify the exact cause of a packet loss because the packet drop rate by the malicious node is comparable to that of wireless link errors. Most of the existing IDS models observe the packet dropping rate to detect the attack at the network layer. However, lack of detecting the causes of packet drops and identifying the attacker nodes responsible for malicious drops in existing works leads to increase the false positives. Clearly, deciding whether a packet drop is intentional or unintentional in a MANET environment is a challenging problem. Incorporating the knowledge of link error due to mobility and congestion levels at neighboring nodes is the primary notion of reducing the false positive and improves the detection accuracy over packet dropping attack [25][26]. The proposed work integrates cross-layer unique features that differentiate the packet loss due to mobility and congestion from the malicious actions in the design of the IDS to distinguish the malicious dropping actions from the dropping due to other network conditions. To achieve this, it retrieves the cross-layer features from Physical, MAC, and Network layers and measures the packet loss induced by the mobility and congestion. The block diagram of CID system is shown in Figure 1.

The CID consists of two major components named as the local detection engine and the IDS. The local detection engine observes the total packet loss in data forwarding phase and differentiates it from the packet loss due to network conditions (packet loss threshold). If the actual packet loss exceeds the packet loss threshold value, the local detection engine enables the nodes to turn on its IDS and to collect the evidence from neighboring nodes using DS theory to confirm the suspected nodes' behavior.

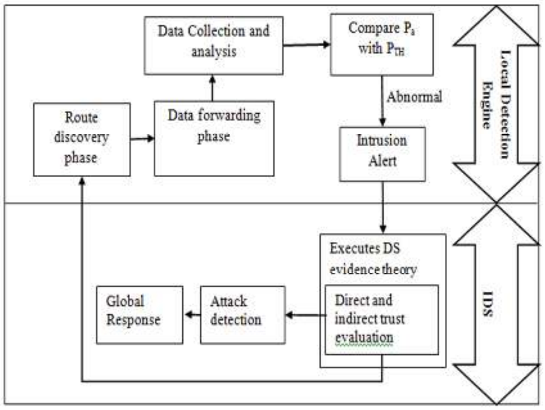

Figure-1: Block Diagram of CID System

3.1 System Model

The network is represented as a communication graph G (N, E). The network G contains a number of mobile nodes, N over a network area X*Y and E contain all directional links between the nodes ∈N. The communication range of a node is represented as R. The speed of each mobile node is S. By persistently observing the actual packet loss probability due to node misbehavior (P_a), the CID system measures the trust values of nodes. The CID fixes a packet loss threshold (P_{TH}) using the packet loss probability due to mobility (P_m) and congestion (P_c) using features retrieved from physical, MAC, and network layer. The CID compares the P_L with P_{TH} to detect the abnormal behavior of nodes. It generates an intrusion alarm to activate the IDS when the abnormal behavior is detected in the network. To confirm the attack behavior, the IDS evaluates trust of the suspected node by collecting evidence from neighboring nodes using DS evidence theory. The DS evidence theory utilizes the belief (Bel (H)) and plausibility (pl(H)) to calculate the trustworthiness of the suspected node.

3.1.1 Attacker model

Consider a malicious node N decides to drop the received packets instead of forwarding them to disrupt the network activities. There are two objectives behind the packet dropping attackers that involve in dropping the received data packets and routing packets such as selfish and malicious. In selfish dropping, the packet dropping attacker does not forward the packets to save its energy. In malicious dropping, the attacker drops the packets in two ways, named as Black and Gray hole. The black hole attackers aim to degrade the network performance by dropping the packets persistently. Instead of dropping all the packets, the gray hole attackers drop some part of packets and disrupts the network functions. If a packet dropping attack happens in the network, the sender node may misunderstand the packet loss might have caused due to a link error. It retransmits the packets repeatedly, resulting in high energy consumption at the sender.

3.2 Local Detection Engine

In the CID, the local detection engine of a node collects its data stream and the data stream from its neighboring nodes in the network, and it analyzes the network traffic in terms of packet loss rate to determine the malicious behavior. To differentiate the packet loss due to malicious behavior from normal network conditions, the CID utilizes the cross layer approach. The CID fixes the packet loss threshold using the features of a physical, MAC, and network layer the link error can be observed using signal strength and Route ERRor (RERR) packet, and congestion due to Ready To Send (RTS) and Clear To Send (CTS) [27].The primary objective of including cross-layer features in packet loss threshold measurement is to identify the malicious behavior and to increase the efficiency of wireless communication. The local detection engine turns on the IDS when observes the malicious behavior of a node.

3.2.1 Observing total packet loss

The packet loss rate is the ratio of the number of packets received to the total number of forwarded packets. The CID measures the total packet loss probability,$P_t$using the number of ACK packets received in the data forwarding phase. The CID computes the total packet loss probability, P_t for every Δt as follows.

$$P_t = 1 - \left\{ {}^{\left(\sum_{x=1}^{n} P_{received}\right)}/_{n} \right\}_{\Delta t} \qquad (1)$$

In equation (1), the $P_{received}$represents the received packets and n represents the total number of forwarded packets for a particular period, Δt. The term Δt is the time difference between two consecutive time intervals, $t_{i,}$and t_{i+1}. Two cases occur in receiving the packets fromreceiver side.

$$P_{received} = \begin{cases} 1; & \text{if } RTT_{delay} < T_{RTT} \\ 0; & \text{Otherwise} \end{cases}$$

The CID utilizes Round Trip Time (RTT) delay assigned to the data packet for receiving an ACK packet. The $RTT_{delay}$is the amount of time taken to forward the data packet, and receive an ACK successfully to the corresponding data packet. The T_{RTT} is the total RTT value assigned to the forwarding data packet. If the $RTT_{delay}$is less than the T_{RTT} value, the packet that is transmitted from one end is received successfully at the receiver end and $P_{received}$= 1. Otherwise, the packets are dropped either due to congestion, mobility, or malicious activity and $P_{received}$= 0.

3.2.2 Defining malicious behavior of a node

The CID considers the packet dropping due to network congestion, mobility, and link error to measure the packet loss threshold and to define the malicious behavior of a node. To define the malicious behavior, the CID takes into account the following two cases.

In the firstcase, the packet loss in MAC layer due to network conditions is considered. For example, node A requires to send packets to a node B. Initially, the node A forwards an RTS message to B and it waits until the medium is free. The RTS message may suffer fromprobability, P_{RTS} by a collision occurred due to another node forwards the RTS message to B at the same time. The B replies to A with a CTS message, when it receives the RTS successfully from A. Otherwise, the CTS message may suffer from a probability; P_{CTS} by a hidden node that is located within the range of B and out of range of A transmits a message to B simultaneously. In general, a CTS collision only occurs if there is no previous RTS collision and thus, the actual CTS collision probability is referred as $(1\text{-}P_{RTS})P_{CTS}$. The packet dropping rate due to congestion is calculated using equation (2).

$$P_c = \{1 - (1 - P_{RTS}) * [1 - (1 - P_{RTS})P_{RTS}]\} \qquad (2)$$

In the second case, the CID estimates packet loss due to mobility, P_m is using the signal strength measurement and RERR. The Received Signal Strength (RSS) of a HELLO packet transmitted between node A and B is measured as follows.

$$RSS = 10\log_{10}\left({}^{k}/_{R^2}\right) \qquad (3)$$

In equation (3) k is the constant and R is the transmission distance. To evaluate the path loss probability (P_m) due to mobility, the CID measures the P_m at each time interval t. The P_m is calculated using equation (4).

$$P_m = \left\{1 - \left({}^{RSS}/_{RSS_{act}}\right)\right\} \qquad (4)$$

In (4), the RSS and RSS_{act}represent the received signal strength occurred and actual received signal strength value, when the communicating devices are located in R distance. There are three cases considered in taking the P_m value into account to measure the packet loss threshold value.

P_m >0; Communicating nodes move far away from each other

P_m =0; Communicating nodes are located in R distance

P_m <0; Communicating nodes move close to each other

If the P_m value is greater than zero, the nodes A and B moves far away from each other, resulting in high packet loss due to node mobility. The nodes A and B are located in R distance when the P_m value is equal to zero. As a result, there is no packet loss occurred due to mobility. If the P_m value is less than zero, the RSS value is high, and there is no packet loss. In the case of observing the poor signal strength of a HELLO packet, the CID enables the routing protocol to instruct the previous hop of a mobile node in a path to send an RERR. The neighboring nodes that overhear the RERR packet decide that the next hop is moved. The CID measures the packet loss happened due to the malicious actions as follows.

$$P_a = P_t - P_c - P_m \qquad (5)$$

$$P_a < P_{TH} \qquad (6)$$

Equation (5) and (6) depict the relationship between the packet loss threshold and a packet loss probability due to malicious actions. The threshold is changed owing to, network conditions such as congestion and mobility for every Δt interval.When the condition of Equation (6) is satisfied, the nodes confirm the malicious behavior of the neighboring node. The corresponding local analyzer generates a local intrusion alert to activate the IDS. The CID starts to compute the trustworthiness using DS evidence theory by providing the value of P_a-P_{TH} as input to the IDS.

3.3 Intrusion Detection System

To reduce the energy consumption, the location detection engine in CID observes the malicious behavior using cross-layerapproach, and it generates an intrusion alert to turn on IDS. The IDS starts to evaluate the trust value of a suspected node in two steps such as direct and indirect. In CID, the IDS takes into account the output of local detection engine i.e. P_a to measure the direct trust value and updates in a trust table of a node. In addition to, the IDS collects the evidence that contains the trustworthiness about the suspected node from its neighbors to measure the indirect trust value and to confirm the attack behavior of the node. Thus, the CID system successfully reduces the false positive in attack detection accuracy.

3.3.1 Evaluating trust on node

The CID evaluates the trust value of a node by observing the recent transaction records using the local detection engine. Using the output of local detection engine that calculates the P_a value of a node at each time interval, the node calculates the Direct Trust (DT_S) value of node S as follows.

$$DT_s = 1 - P_a \qquad (7)$$

Each node stores the DT value in a trust table. In MANETs, the absolute trust cannot always provide a comprehensive evaluation of the suspected node, as it may compromise its local detection engine to report it falsely as benign. The CID instructs the IDS to collect evidence from its neighboring nodes that are used to provide auxiliary information to confirm the malicious behavior of the suspected node.

3.3.2 Evaluating indirect trust using DS theory

Each node keeps a trust table that associates its trust value and neighboring nodes. The trustworthiness of a neighbor node is not distributedglobally but keeps it local. When the neighboring nodes receive an intrusion alerts, it shares their observations as evidence to the corresponding node that generates an intrusion alarm. The neighboring nodes may be compromised due to routing attacks, and it provides numerous uncertain evidence to the node that generates the intrusion alert. To avoid this, the CID enables the IDS to utilize the belief and plausibility of a hypothesis (either real or malicious event) for identifying the evidence of trusted nodes. The CID measures the trust value regarding direct and indirect, which is determinedby limited trustworthyevidence for overall trust evaluation.

Consider the nodes A and S are neighbors and the local detection engine of node A and S identifies that the node S is suspected. If a node S fails to generate an intrusion alert to prove that a node S is a suspected node, the node A generates an alert for node S after waiting for t time. Node B, C, D are the neighboring nodes of node A and S. Node B and C claims about node S is a suspected one, but node D claims the node S as a legitimate node. The CID estimates the belief of a Hypothesis H and H^, where H is a hypothesis that node S is a suspected node and H^ is the hypothesis "not H". The belief of neighboring nodes B and C on H (Bel(H)) and the belief of node D on H^ (Bel(H^)) are estimated as follows.

$$\mathrm{Bel}(H) = \sum_{H_i \subset H} m(H_i) / |H_i| \qquad (8)$$

$$\mathrm{Bel}(H\hat{}) = \sum_{H_j \subset H} m(H_j) / |H_j| \qquad (9)$$

In the equation (8) and (9), i denotes the set of nodes that claim node S as trustworthy (node B and C), and j denotes the set of nodes that claim node S is malicious (node D). To reduce the false positives, the IDS estimates trustworthiness of the neighboring nodes that provides evidence for H be true, named as Plausibility (Pl). The Pl is calculated for each hypothesis as shown in the equation (10).

$$\mathrm{Pl(H)} = 1 - \left\{ \prod_{\mathrm{H_i \subset H}} (1 - \mathrm{DT_i}) \right\} \qquad (10)$$

The CID takes both the belief and plausibility values of hypothesis to estimate the Total trust on Hypothesis, $T_t(H)$. The IDS evaluates the $T_t(H)$ as follows.

$$\mathrm{T_t(H)} = {\{\mathrm{Bel(H)} * \mathrm{Pl(H)}\}}\Big/{\left\{1 - \left(\mathrm{Bel^\wedge(H)} * \mathrm{Bel^\wedge(H^\wedge)}\right)\right\}} \qquad (11)$$

In case, if the node j is compromised by a suspected node S and falsely report about it, the CID identifies the false report of nodes Є j using Equation (11) and excludes its opinion in measuring the trust value of node S. Likewise, the CID includes only evidence of nodes Є i in indirect trust evaluation and improves the attack detection accuracy.

3.3.3 Total trust evaluation

It is necessary to calculate the average trust for deciding the trustworthiness of a suspected node. The average trustworthiness of node S is calculated using direct and indirect trust values. The IDS takes the DT_S and the evidence collected from the trustworthy neighbors as inputs to calculate the trustworthiness of the node S. The total trust on believing the node S as trustworthy, $T_t(S)$ is estimated as follows.

$$\mathrm{T_t(S)} = {\left\{ \mathrm{DT_S} + \sum_{\mathrm{X=1}}^{|\mathrm{i}|} {(\mathrm{DT_S})_\mathrm{X}}\Big/{|\mathrm{i}|} \right\}}\Bigg/{2} \qquad (12)$$

In equation (12), The $(DT_S)_x$is the trust value of S provided by trusted neighbor nodes Є I. The value of $T_t(S)$ denotes the level of malicious behavior of node S. The CID system effectively detects and mitigate the intruder from the network. Integrating the CID system, the topology based routing protocol takes into account the $T_t$value of routers in selecting the routing path over MANET and improves the routing performance.

4. EXTENDING CID IN AODV ROUTING PROTOCOL

The proposed CID system is extended with the AODV routing protocol to detect routing attacks. Each node in MANET preserves and maintains information about routing and neighboring nodes in a table. The CID has three phases such as route discovery, route maintenance, and data forwarding.

The CID adds a new field, named as trust field into a node's routing table. Each node periodically record and updates the trust values of neighboring nodes based on the behavior of neighbors in the data forwarding for every time interval. The nodes exploit the trust information in the route discovery phase. Each node rebroadcasts the RREQ that is forwarded by a highly trusted node. The destination exploits the trust value of intermediate nodes in the RREQ to select a highly trusted routing path. The data forwarding phase of CID is the same as in AODV.

In route maintenance phase of CID, the intermediate node sends an RERR message, when a link error occurs in the active path due to mobility. There are two cases observed in route maintenance phase of the CID. In the first case, the broken link is closer to the source node than to the destination; the intermediate node sends an RERR message immediately backward to alert its precursors about the link failure. The precursors stop the data packet forwarding and participate in transmitting the RERR messages. As a result, there is no packet loss due to mobility. If any packet loss happened in the first case, the CID considers the packet loss only happened due to either congestion or malicious activities. There is no need to measure the packet loss due to node mobility. In the second case, the broken link is closer to the destination, and the intermediate node tries to perform a local repair of the route, by sending an RREQ message like the source node. The node with a broken link waits a certain time to discover an alternate route and it unable to forward the receiving messages from its precursors. As a result, the node drops the packets and behaves in a similar way that an attacker. The CID identifies the packet loss happened due to mobility and reduces the false positives in detection accuracy. Thus, the CID increases the routing protocol performance over malicious network traffic.

5. PERFORMANCE EVALUATION

The CID routing protocol is compared with the existing EAACK [24] for analyzing the performance. The efficiency of the CID substantiates through NS-2 simulation. The simulation setup parameters are shown in Table 1.

5.1.1 Simulation Setup

Table-1: Simulation Model

Network Area	1000mx1000m
Number of Nodes	100
Communication Range	250m
Node Mobility	20 m/s
Node Energy	4 Joules
Packet Size	512 bytes
Data Rate	2 Mbps
Routing protocol	CID
Interface Type	Phy/WirelessPhy
MAC Type	802.11
Queue Type	Droptail/PriorityQueue
Queue Length	100 packets
Antenna Type	TwoRayGround
Transport Agent	TCP
Application Agent	CBR
Simulation Time	100seconds

5.2.2 Simulation Results

The simulated results discuss the different simulation scenarios to facilitate the performance of the CID routing protocol under various performance metrics such as Intrusion Detection Accuracy, Remaining energy level, False alarm rate, Throughput, and Conflict clearance.

- Intrusion Detection Accuracy - Intrusion Detection Accuracy is the ratio of the number of identified intruders to the total number of intruders.
- Remaining Energy Level - It refers the average remaining energy of the nodes.
- False Alarm Rate - It is the ratio of the number of false alarms to the total number of alarms generated over time.
- Throughput -It is the rate of successful data delivery.
- Conflict Clearance - It is the ratio of correctly identified false evidence to the total number of false evidence.

5.2.1 Impact of number of attackers

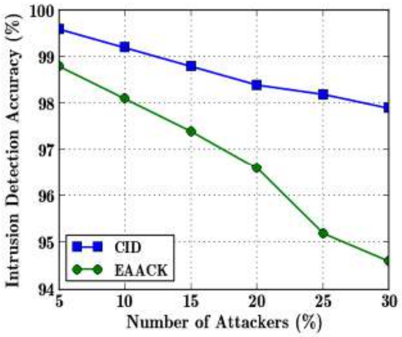

Figure-2: Number of Attackers Vs Intrusion Detection Accuracy

Figure 2 demonstrates the intrusion detection accuracy results of both the CID and EAACK for the various numbers of attackers over a 100 node topology. In both systems, the intrusion detection accuracy is decreased by increasing the number of attackers from 5% to 30%, as the high number of attackers provides the uncertain evidence about the node. For instance, the CID decreases the intrusion detection accuracy by 1.7%, when varying the attackers from 5% to 30%. The CID determines the attackers using optimal packet loss threshold that is estimated using the features of physical, MAC, and network layers and confirms the malicious behavior using strong evidence, collected only from trustworthy neighbors. On contrast, the existing EAACK determines the attackers using only ACK packets. Thus, the CID attains high detection accuracy, when compared to EAACK. In Fig. 2, at the point of 25% of intruders, the CID increases the detection accuracy by 3% more than that of EAACK.

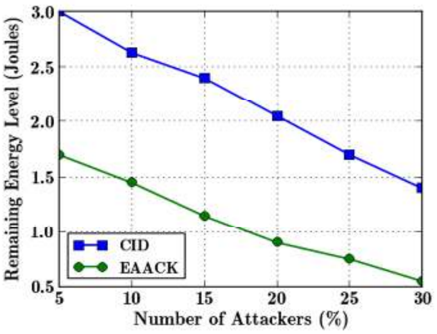

Figure-3: Number of Attackers Vs Remaining Energy Level

Figure 3 illustrates the energy level results of both the CID and the EAACK. In CID, the IDS calculates the trustworthiness value of attackers using DS evidence theory and confirms the attack behavior based on recommendation trust. If the numbers of attackers are high in the network, the IDS requires high energy to collect evidence and perform computational calculations. So, the remaining energy level of CID is decreased, when increasing the number of attackers. For instance, in Fig. 3, the CID decreases the remaining energy level by 53%, when varying the attackers from 5% to 30%. However, the energy utilization level of CID is minimum, compared to EAACK as the CID activates IDS when only the intruders present in the network. At the point of 10% of attackers, the CID attains high remaining energy level by 42% more than that of EAACK.

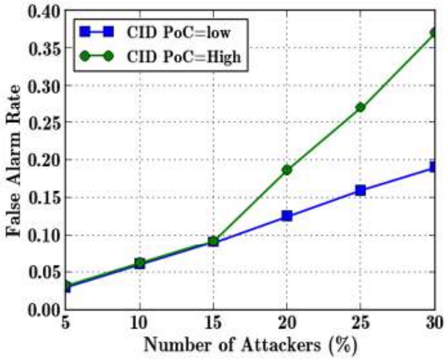

Figure-4: Number of Attackers Vs False Alarm Rate

Figure 4 shows the results of false alarm rate of CID by varying the attackers, and the false alarm rate is evaluated for low and high Probability of Congestion (PoC) values. For low and high PoC, the CID attains same false alarm rate, when varying the attackers from 5% to 15%, as it accurately identifies the packet loss happened by malicious behavior using optimal packet loss threshold that is fixed using the RTS and CTS loss probability in the MAC layer. At congestion scenarios, the CID may suspect the legitimate nodes and the false alarm rate is suddenly increased. In Fig. 4, for high PoC, the CID increases the false alarm rate by 72%, when varying the attackers from 15% to 30%.

5.2.2 Impact of malicious behavior

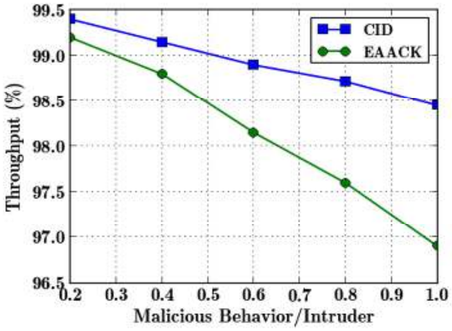

Figure-5: Malicious Behavior/Intruder Vs Throughput

Figure 5 shows the results of throughput of both the CID and the EAACK by varying the malicious behavior of an intruder from 0.2 to 1. Both the protocols decrease the throughput with the increasing malicious behavior of a node. As the node with a high malicious behavior did not cooperate in routing, it drops a large number of packets. For instance, the CID decreases the throughput by 0.9%, when varying the malicious behavior of a node from 0.2 to 1. However, the CID attains high throughput more than that of EAACK as the CID selects high trustworthy nodes in collecting evidence and in route discovery. At the point of malicious behavior of 0.8, the CID attains high throughput to 1.12%, compared to EAACK.

5.2.3. Impact of traffic rate

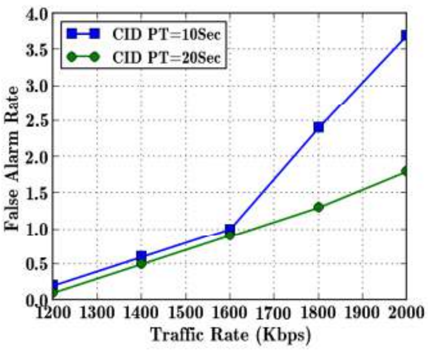

Figure-6: Traffic Rate Vs False Alarm Rate

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

By varying the traffic rate from 1000 Kbps to 2000 Kbps, the false alarm rate of CID is evaluated for various Pause Time (PT) values such as 10 and 20 seconds as shown in Fig. 6. The CID maintains the nearly equal false alarm rate for low and high PT values when varying the network traffic from 2000 Kbps to 1600 Kbps. However, the CID suddenly increases the false alarm rate, when it reaches the saturation point of 1600 Kbps. After the saturation point, the nodes drop a high number of packets due to congestion and mobility and the CID cannot differentiate the packet loss due to malicious behavior from harsh channel conditions. Thus, increases the false alarm rate. For PT=10 seconds, the CID suddenly increases the false alarm rate by 72%, when varying the traffic rate from 1600 Kbps to 2000 Kbps.

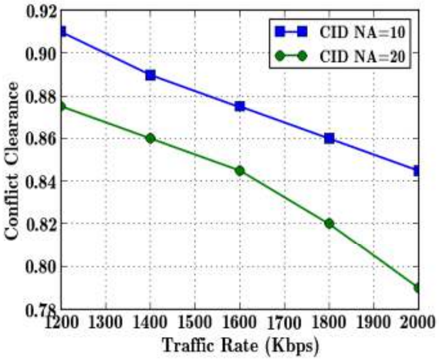

Figure-7: Traffic Rate Vs Conflict Clearance

Figure 7 depicts the conflict clearance results of CID, by varying the traffic rate and Number of Attackers (NA). The CID decreases the conflict clearance when varying the traffic rate from 1000 Kbps to 2000 Kbps. After the saturation point of 1600 Kbps, the nodes drop a high number of packets due to congestion, mobility, and malicious activities, and so the CID cannot collect adequate, correct evidence for evaluating the trustworthiness of a node. Thus, reduces the conflict clearance while increasing the traffic rate and a number of intruders. For NA=10, the CID attains 0.91 conflict clearance at the point of 1200 Kbps of traffic rate but is decreased to 0.875, when NA=20.

6. CONCLUSION

This work has proposed CID with the objective of packet dropper identification with considerable energy consumption using cross layer information. The CID acquires truthful packet-loss information due to the malicious actions on individual nodes by exploiting the cross layer information obtained from network, MAC, and physical. It includes the components of local detection engine and the IDS to determine packet dropping attacks. By differentiating the packet loss due to malicious activities from harsh channel conditions using cross-layer features, the local detection engine supports the IDS to improve detection accuracy. As the local detection engine only triggers the IDS, when it detects the malicious behavior in the network, the CID system significantly reduces the routing overhead and energy consumption. To further improve the detection accuracy, the CID system collects trustworthy evidence using DS theory and enhances the routing performance, while extending with the AODV routing protocol. Finally, the simulation results show that the CID detects the packet dropping attacks with high detection accuracy and considerable energy consumption.

REFERENCES

[1] Chlamtac, Imrich, Marco Conti, and Jennifer J-N. Liu "Mobile ad hoc networking:imperatives and challenges", Ad hoc networks , Vol.1, No.1, pp.13-64, 2003.

[2] De Morais Cordeiro, Carlos, and Dharma P. Agrawal "Mobile ad hoc networking", Center for Distributed and Mobile Computing, pp.1-63, 2002.

[3] Zhang, Yongguang, Wenke Lee, and Yi-An Huang, "Intrusion detection techniques for mobile wireless networks", Wireless Networks, Vol. 9, No.5, pp. 545-556, 2003.

[4] Chen, Thomas M., and VaradharajanVenkataramanan, "Dempster-Shafer theory for intrusion detection in ad hoc networks", IEEE Internet Computing, Vol.9, No.6, pp.35-41, 2005.

[5] Fung, Carol, "Collaborative intrusion detection networks and insider attacks", Ubiquitous Computing, and Dependable Applications, Vol.2, No.1, pp.63-74, 2011.

[6] Fung, Carol J., et al, "Dirichlet-based trust management for effective collaborative intrusion detection networks", IEEE Transactions Network and Service Management, Vol.8, No.2, pp.79-91, 2011.

[7] Sen, Jaydip, “A robust and fault-tolerant distributed intrusion detection system”, Parallel Distributed and Grid Computing (PDGC), pp.123-128, 2010.

[8] A Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, and H. Mouftah, “AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement”, 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 634- 640, 2010.

[9] Mohammed, Noman, HadiOtrok, Lingyu Wang, MouradDebbabi, and Prabir Bhattacharya, “Mechanism design-based secure leader election model for intrusion detection in MANET”, IEEE Transactions Dependable and Secure Computing, Vol.8, No. 1, pp.89-103, 2011.

[10] P.Yi, Z.Dai, Y. Zhong and S.Zhang, “Resisting Flooding Attack in Ad Hoc Networks”, Proceedings of IEEE International Conference on Information Technology Coding & Computing ITCC, 2005.

[11] Ping, Yi, Jiang Xinghao, Wu Yue, and Liu Ning, “Distributed intrusion detection for mobile ad hoc networks”, Systems Engineering and Electronics, Vol.19, No.4, pp.851-859, 2008.

[12] Sterne, Daniel, PoornimaBalasubramanyam, David Carman, Brett Wilson, Rajesh Talpade, Calvin Ko, RavindraBalupari, C-Y. Tseng, and T. Bowen, “A general cooperative intrusion detection architecture for MANETs”, Third IEEE International Workshop, pp. 57-70, 2005.

[13] Huang, Yi-an, and Wenke Lee, “A cooperative intrusion detection system for ad hoc networks”, Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp.135-147, 2003.

[14] K.Sanzgiri and M.Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks”, Proceedings of IEEE International Conference on Network Protocol (ICNP’ 02), pp.78-87, 2002.

[15] Y.Hu, B. Johnson and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks”, International Journal of Ad hoc Networks, Vol.1, No.1, pp 175-192, 2003.

[16] N. Stakhanova, S. Basu, W. Zhang, X. Wang, and J. Wong, “Specification Synthesis for Monitoring and Analysis of MANET Protocols”, Proceedings of International Symposium on Frontiers in Networking with Applications, 2007.

[17] G.F.Cretu, J.Parekh, K.Wang and S.J.Stolfo, “Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks”, Proceedings of IEEE Consumer Communication and Networking Conference, 2006.

[18] Y. Liu, C. Comaniciu and H. Man, “Modeling Misbehavior in Ad Hoc Networks: a Game Theoretic Approach for Intrusion Detection”, International Journal of Security and Networks, Vol.1, No.3, pp. 243 - 254, 2006.

[19] H.Jiang and H.Wang, “Markov Chain Based Anomaly Detection for Wireless Ad-Hoc Distribution Power Communication Networks”, Proceedings of IEEE Power Engineering Conference, pp.1-249, 2005.

[20] A.Nadeem and M.Howarth, “Adaptive Intrusion Detection & Prevention of Denial of Service Attacks in MANETs”, Proceedings of ACM International Wireless Communication and Mobile Computing Conference (IWCMC 09), pp.926-930, 2009.

[21] 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.

[22] A.Mitrokosta, N.KomninosandC.Douligeris, “Intrusion Detection with Neural Networks and Watermarking Techniques for MANETs”, Proceedings of IEEE International Conference on Pervasive Services, pp.118-127, 2007.

[23] Liu, Kejun, et al, “An acknowledgment-based approach for the detection of routing misbehavior in MANETs”, Mobile Computing, IEEE Transactions, Vol.6, No.5, pp.536-550, 2007.

[24] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami, “EAACK—A Secure Intrusion-Detection System for MANETs”, IEEE Transactions, Vol.60, No.3, pp.1089-1098, 2013.

[25] Shrestha, Rakesh, Kyong-Heon Han, Dong-You Choi, and Seung-Jo Han, “A novel cross layer intrusion detection system in MANET”, In Advanced Information Networking and Applications (AINA), 24th IEEE International Conference, pp. 647-654, 2010.

[26] Sánchez-Casado, Leovigildo, Gabriel Maciá Fernández, and Pedro Garcıa-Teodoro, "Multi-Layer Information for Detecting Malicious Packet Dropping Behaviors in MANETs", 2012.

[27] Shu, T., &Krunz, M, "Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing", In Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, pp. 87-98, 2012.