Intrusion Detection Scheme in Secure Zone Based System

[1]Susan Bandecchi and [2]Nicoleta Dascalu
[1,2] Division de Natural Science, Universidad de Sonora, Hermosillo, Son., Mexico.
[1]susanbandecchi@protonmail.com

Article Info
Journal of Computing and Natural Science (http://anapub.co.ke/journals/jcns/jcns.html)
Doi: https://doi.org/10.53759/181X/JCNS202101005
Received 22 October 2020; Revised form 28 November 2020; Accepted 29 December 2020.
Available online 05 January 2021.

Abstract – Mobile Ad hoc Networks (MANETs) are short lived networks that are greatly utilized in many applications such as special outdoor events, for communications in regions having no wireless infrastructure as in natural disasters, military operations, mine site operations and urgent business meetings. The self-organizing properties of its nodes forming the network are rapidly deployable and possess no infrastructure. Hence securing MANETs is a primary concern due to the absence of a central infrastructure and node mobility for which Intrusion Detection System (IDS) has been adopted in addition to the primary lines of defence such as cryptography and authentication. A Hierarchical IDS, namely, the Zone based IDS, functions in MANETs based on node collaboration and detects network layer intrusions with better accuracy. The proposed Cross Layer Detection in cohesion with anomaly detection technique of Zone based IDS aids in detecting attacks originating from the deeper layers of protocol stack, namely, physical and MAC layer thus providing better monitoring and improving the detection accuracy in Zone based IDS. The simulation results showcase an effective increase in detection rates and reduced false positives.

Keywords – MANET, IDS, Zone based IDS, Physical layer, MAC layer, network layer, Cross layer intrusion detection, detection rate, false positive rate, trust.

I. INTRODUCTION

An ad hoc network is a multihop network which comprises of many nodes formed temporarily to meet a specific purpose. These networks do not rely on any centralized infrastructure and is dynamic in order to support mobility. Self-organization and adaptation are the two properties that play a vital role in the ad hoc network. The friendly nature of every node is required to build a self-configurable environment and thereby the nodes help to transmit messages in order to reach the destinations. In other words, mobile hosts act as both receiver and transmitter to forward messages among one another in a Mobile Ad hoc Network (MANET) since there is no static infrastructure. Also the hosts (nodes) in the network leave or join the network and they adapt themselves to the networking environment [1].

There are several challenges in the Mobile Ad hoc network since it is an emerging technology. The foremost application of these networks were in the military tactical operations. Still there lays the limitation posed by necessity of infrastructure such as base station, allocation of frequencies to meet the demand of users etc. In order to mitigate these limitations, various studies and approaches have been introduced like frequency reuse concepts, clustering techniques, sectoring techniques, and assignment of conflict free channels to meet the user desires. Yet the wireless communication potential in MANETs is not fully utilized. These wireless networks inherit the traditional problem of wireless and mobile communication such as bandwidth optimization, power control and transmission quality enhancement. Some of the major issues of ad hoc networks are given as below [2]:

- Highly Dynamic Topology
- Routing in Mobile Ad hoc Network
- Security in Mobile Ad hoc Network
- IP Configuration in Mobile Ad hoc Network
- Battery Backup Problem

Among these challenges, imparting security to ad hoc networking has always been the biggest challenge and is the focus of research. Security is a primary concern because ad hoc networks lack fixed backbone to regulate networking operations. The dynamic topology causes the nodes to join or leave the network. They are mobile and therefore can be compromised by adversaries to cause security violations. Like any other information systems, Mobile Ad hoc networks also need to preserve the following for its proper functioning and organization, namely, availability, confidentiality and integrity. Primary security methods like firewalls, cryptographic techniques as in encryption; decryption and authentication procedures can be applied. But these measures form only the first layer of defence against security violations in an ad hoc networking environment. So Intrusion Detection Systems (IDS) were designed and developed to play the second layer of defence. For example, when a node or the whole network is attacked, the attacker must break in the IDS and then alter the cryptographic information to pose a threat against a trusted user or the whole system. The role of intrusion detection is more significant in such a way that any attack or intrusions must be detected by the IDS during its occurrence in real time or it should detect the symptoms of any attack or intrusion before the same takes place.

It is a great challenge to design and maintain a system both technically and economically to avoid the attacks since there are various security vulnerabilities. The solution to the problem cannot depend on a single technique or defensive line. An Intrusion Detection System (IDS) is greatly considered to be one of the best solutions for the protection of today's network systems. The research reported by Anderson followed by Denning's seminal paper helps many researchers to do their research in current intrusion detection prototypes. It also extends the research towards wired network IDSs. Though various detection techniques and architecture for host machines and wired networks have been proposed, it should be commonly developed and be applicable on ad hoc network platform. Due to the rapid growth of technology, attacks may also increase which in turn advances several intrusion detection systems. Though every proposed system has its own peculiar feature, the basic concepts remain the same.

A generic architecture of IDS which the monitored system is the area which may be a single host or the whole network that needs protection. The output from the monitored system is fed to the audit collection /storage where data are collected to identify the events and to process in a proper way. The heart and mind of IDS is the processing unit where the algorithms are applied on data for detecting the evidence of suspicious behaviour. Whenever a suspicious intrusive event is detected, an alarm is set. Depending on the IDS architecture, the problems are mitigated by taking appropriate action. The alarm signal, in turn, is fed back to the Site Security Officer (SSO) which takes step against the attack [3].

IDS in MANETs have two fundamental concepts i.e. Intrusion Detection Techniques and Intrusion Detection (ID) Architecture. Intrusion Detection technique is the means of applying certain algorithms to the audit input data to identify detections. The Intrusion Detection Architecture, on the other hand, employs an efficient IDS module along with other modules in order to make a decision for the network nodes to get collaborated and work securely. In wireless networks, collaboration or exchange of data should be done periodically in order to decide intrusion detection effectively. Hence, an ID architecture plays a vital role for defining the various nodes' role and communication among the nodes. Generally, the intrusion detection technique does not depend on the architecture or environment. In a fair manner, anomaly or misuse detection can be adopted in wireless environment as like in wired network in which the differentiation can be done on input audit data given to the algorithm. However, most IDS in MANET utilize anomaly detection because it has the ability to detect unknown attacks as well [4].

Zone Based Intrusion Detection System (ZBIDS)

A Hierarchical and non-overlapping Zone-Based Intrusion Detection System (ZBIDS) architecture was developed. The intrusion detection method used is Markov chain anomaly technique. The routing protocol employed for this framework is Dynamic Source Routing (DSR) Protocol [5]. Two types of nodes exist in this architecture for communicating, namely, the interzone and intrazone. Interzone node connects one zone to another zone. It is also known as the gateway node. The ZBIDS may comprise of two or more gateway nodes. Intrazone nodes are the nodes present within a zone. There is a local IDS agent attached to the intrazone nodes. These nodes effectively monitor anomalies and periodically sent the alerts to the interzone node. The interzone nodes aggregate the alerts and deeply analyze those to generate alarms. In other words, the interzone nodes and intrazone nodes in the zone-based IDS function in unison and play vital roles in collecting, analyzing and sharing the occurrence of any intrusive behavior to its neighboring nodes with the aid of Markov based anomaly detection algorithm. The performance and efficiency of ZBIDS was measured using parameters like Mean Time-To-First Alarm, False Positive Ratio, Detection ratio and Link change rate. The renowned attack occurring in network layer, called the route disruption attack was used for the study to determine intrusions. It was observed that the rate of False positives has been considerably reduced by the ZBIDS [6].

EAACK in ZBIDS

This act may also be due to the lack of cooperation among nodes. In such circumstance, the absence of acknowledgement or packet is mistaken as a sign of misbehaving or intrusion by the ZBIDS. Hence, to further enhance the monitoring effectiveness in ZBIDS, it is proposed that the EAACK scheme can be combined with the Markov anomaly scheme of ZBIDS so as to include selfish nodes during the intrusion detection phase [7]. Selfish nodes are nodes which do not intend to participate in any network routing activities so as to secure its limited resources such as battery power. It is likely that the selfish nodes does not forward the packets or simply drop them without further involvement. In such cases, the intrazone and interzone node, may monitor and tag this behaviour to be malicious or broken thus causing an indication of false positive [8]. Hence, the solution to reduce false positives occurring as per this scenario, is to include an acknowledgement based IDS scheme known as Enhanced Adaptive

Acknowledgment (EAACK) into the existing anomaly scheme of ZBIDS and develop a new algorithm. This would enhance the performance of alert and alarm generation and also reduce the false positives [9].

Fig. 1. Depicts the workflow of EAACK algorithm in intrazone nodes. The EAACK scheme has the Secure ACK (S-ACK) mode and the MRA (Misbehaviour Report Authentication) mode to detect misbehaving nodes in the route [10]. The EAACK scheme ensures that packets reach the destination using an alternate route if acknowledgement or packet drops results. This drop may be caused either by a selfish node that shows no involvement during routing or a malicious node or network congestions. However, the gateway node should not wrongly tag a selfish node as malicious and exclude it away from the zone. In this way, false positives can be reduced more.

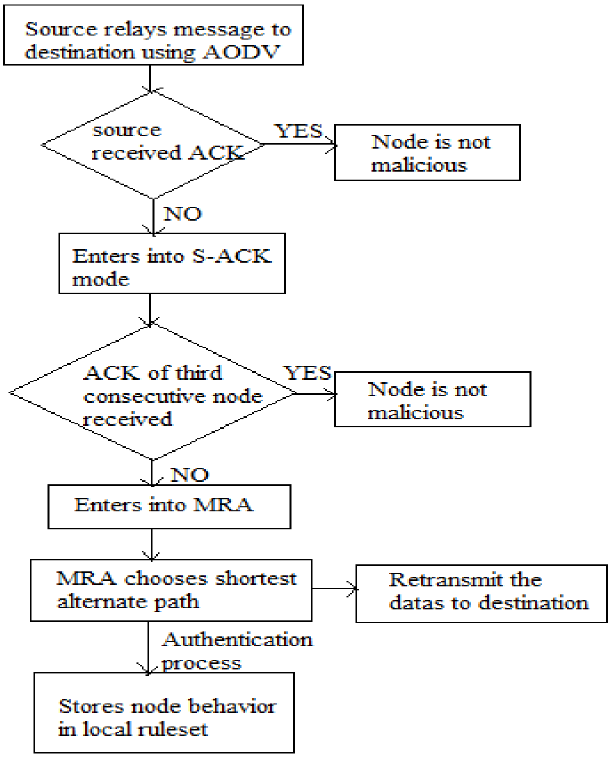
Source relays message to destination using AODV
source received ACK
YES
Node is not malicious
NO
Enters into S-ACK mode
ACK of third consecutive node received
YES
Node is not malicious
NO
Enters into MRA
MRA chooses shortest alternate path
Retransmit the datas to destination
Authentication process
Stores node behavior in local ruleset

Fig 1. EAACK processing in intrazone

Secured and Anonymous ZBIDS (SAZIDS)

The SAZIDS introduces a group signature key algorithm to produce anonymity in ZBIDS. This objective is to exercise a secure communication due to the risk of interzones and intrazones being captured or compromised [10]. Also there may occur chances where the ZBIDS communication can be hindered by delaying and jamming.

This is achieved by introducing the Anonymous Location-Aided Routing [11]. The Anonymization is acquired as follows: A Group signature scheme is a public key signature scheme where the intrazone nodes and interzone nodes may sign a message on behalf of the group. For this, the Group Manager (GM) initializes a set of legitimate nodes in MANET for the SAZIDS offline. The nodes then create their unique private key for producing the group signature. The private key is not disclosed to other nodes including the Group Manager. The nodes also create a corresponding public key and shares with the GM. The Group manager provides a common group public key (PKGM) to verify the group signatures.

To initiate information exchange between the zone members, a Location Announcement Message (LAM) is broadcasted. LAM contains the timestamp, the location coordinates of each node, the temporary public-private key-pair active for that time slot and a group signature calculated over these fields. For every LAM broadcast, the nodes make sure that previous LAM along with timestamp and group signature matches with the new LAM and then rebroadcasts to its neighbors. Gradually a node connectivity graph is built by each node. When a node wishes to communicate with another node belonging to different zone, the source node sends the message encrypted by the session key to the recipient known by its TempID which is a concatenation of present location and group signature. The session key is in turn encrypted using the current Public Key of the recipient as reported in its recent LAM. When the node receives the message, it first recovers the session key and then uses it to decrypt the message.

The overall evaluation of SAZIDS as performed in the NS2 simulation environment proves that this method can guarantee the secured and reliable transmission of data values without involvement of malicious activities.

II. LAYER INTRUSION DETECTION (LID)

Security is an important challenge in MANETs that addresses detecting intrusions by monitoring the MAC layer in addition to the Network layer. The idea is to extend the function of SAZIDS to detect intrusions using cross layer information [12]. The SAZIDS architecture is extended to support cross layer design to exchange information and improve the overall network performance. By extending SAZIDS, packet dropping attacks may be detected with proper cause. This can be achieved without much energy consumption over the malicious traffic and reducing the false positives. The channel conditions in MAC play a vital role for transferring packets.

The packet dropping attack is the troublesome network layer threat in MANETs [13]. Instead of forwarding the received data, the attackers maliciously drop the packets and disrupt the normal operation of the network. Most of the existing IDS models observe the packet dropping rate to detect the attack only at the network layer. Incorporating the knowledge of link error due to mobility and congestion levels at neighbouring nodes is one of the primary notion for reducing the false positives and improving the IDS detection accuracy. The proposed study integrates cross-layer unique features in the design of the IDS to distinguish malicious actions from dropping due to network conditions. This can be achieved by retrieving the cross-layer features from Physical, MAC and Network layer.

The CLID consists of two major components namely the IDS and the local detection engine. 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 neighbouring nodes using DS theory to confirm the suspected nodes' behaviour.

Network Model

The network is represented as a communication graph G (N, E) [14]. The speed of each mobile node is S. The communication range of a node is represented as R. By persistently observing the actual packet loss probability due to node misbehaviour (Pa), the CLID system measures the trust values of nodes. The CLID fixes a packet loss threshold (PTH) using the packet loss probability due to mobility (Pm) and congestion (Pc) using features retrieved from physical, MAC, and network layer. The CLID compares the PL with PTH to detect the abnormal behaviour of nodes..

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 namely 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 hole 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 grayhole 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.

III. RESULTS AND DISCUSSION

NS-2 simulator tool is utilized to compute the performance of the proposed Cross Layer Intrusion Detection System (CLIDS). The simulations model a network comprises of 100 nodes placed randomly within a 100 × 100 meters area. The simulation parameter values utilized in this study are given in Table 1.

Table 1. Simulation Parameters

Simulation Parameters	Value
Channel	Wireless Channel
MAC	802.11
Antenna Type	Omni Antenna
Routing Protocol	AODV
Initial Energy	100 Joules
Traffic Type	CBR

Simulation Parameters	Value
Agent	UDP
Simulation Area	100x100 meters
Number of Nodes	100

Delivery Ratio

Delivery ratio of the proposed framework is improved than the existing Zone based IDS. The variation of delivery ratio parameter in comparison to the different studies performed is depicted in Fig. 2.

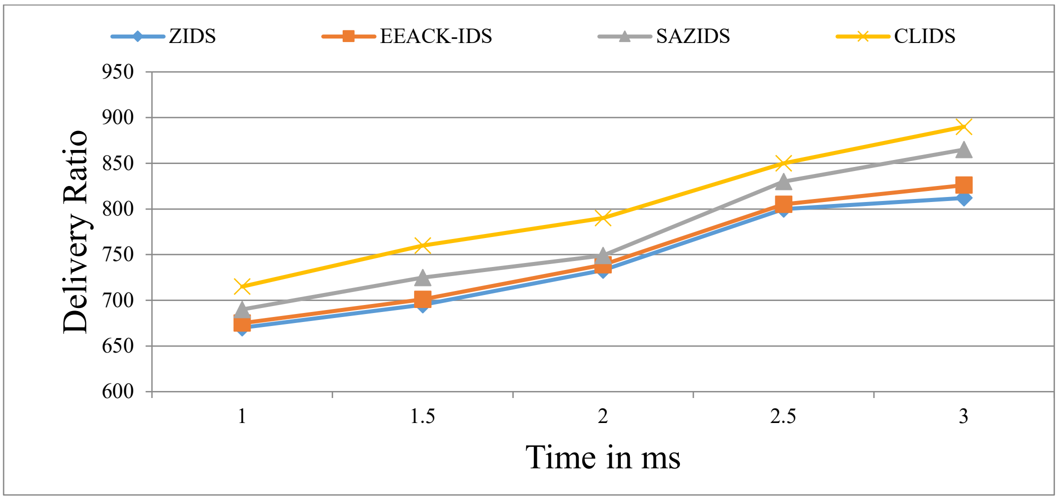

Fig 2. Packet Delivery Ratio

It can be studied from Fig. 2. that the proposed method, CLIDS can forward more number of packets to the destination when compared to the existing ZBIDS and the proposed work EEACK-IDS and SAZIDS. CLIDS ensures 3.78% better performance than SAZIDS, 7.95% improved outcome than the existing system ZBIDS and6.91% improved delivery rate than the EEACK-IDS.

Detection Rate

The detection rate of the proposed work is outlined in Fig. 3.

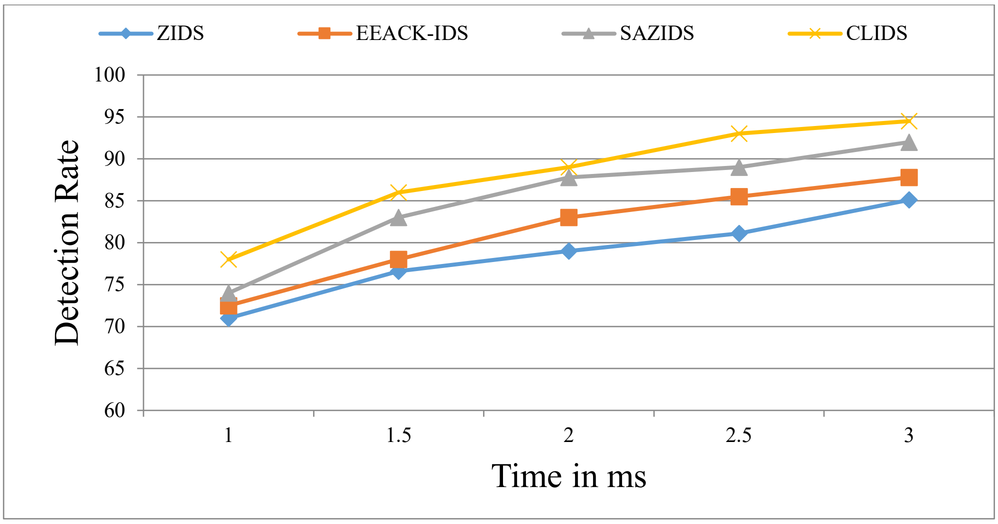

Fig. 3. Detection Rate Comparison

The Fig. 3. reveals that the proposed system CLIDS can identify the attack more accurately than the existing detection strategy ZBIDS, EEACK-IDS and SAZIDS. CLIDS exhibits 3.45% better performance than the SAZIDS, 12.14% enhanced outcome than the current strategy ZBIDS and 8.28% better detection rate than EEACK-IDS.

False Alarm Rate

The examination of false alarm rate is shown in Fig. 4. The proposed CLIDS can reduce the false alarm rate than the existing exploration method ZBIDS, EEACK-IDS and SAZIDS. CLIDS shows 18.18% better performance than SAZIDS, 17% better performance than EEACK-IDS and 10.95%.

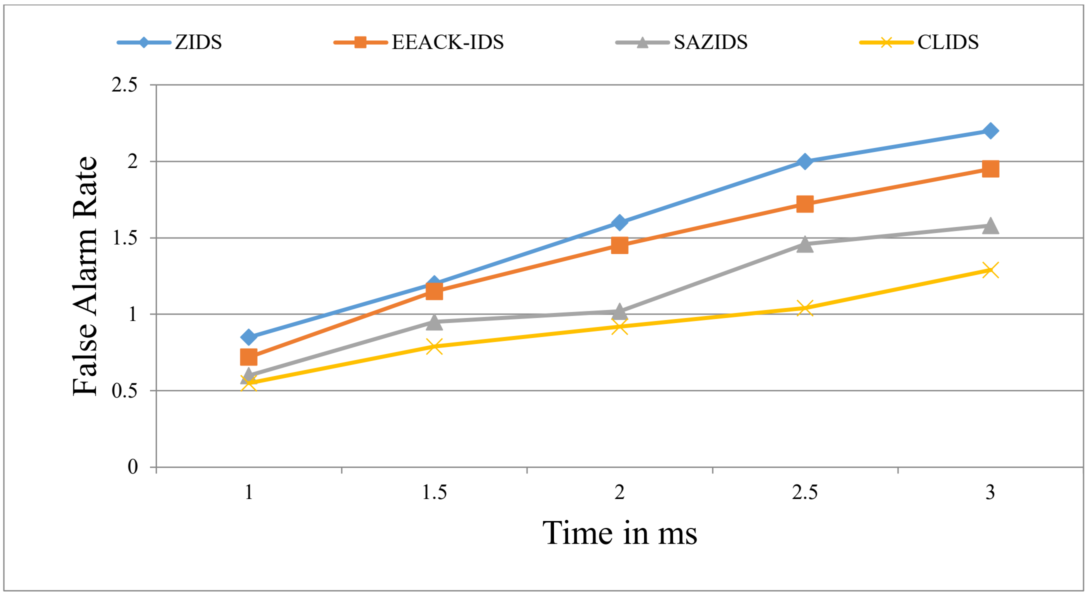

Fig. 4. False Alarm Rate Comparison

Link Change Rate

Fig. 5. presents the assessment of link change rate. It is foud that CLIDS can reduce the link change rate than the current ZBIDS, EEACK-IDS and SAZIDS. CLIDS shows 16.16% better performance than SAZIDS, 45.8% enhanced outcome than ZBIDS and 44% better performance than EEACK-IDS.

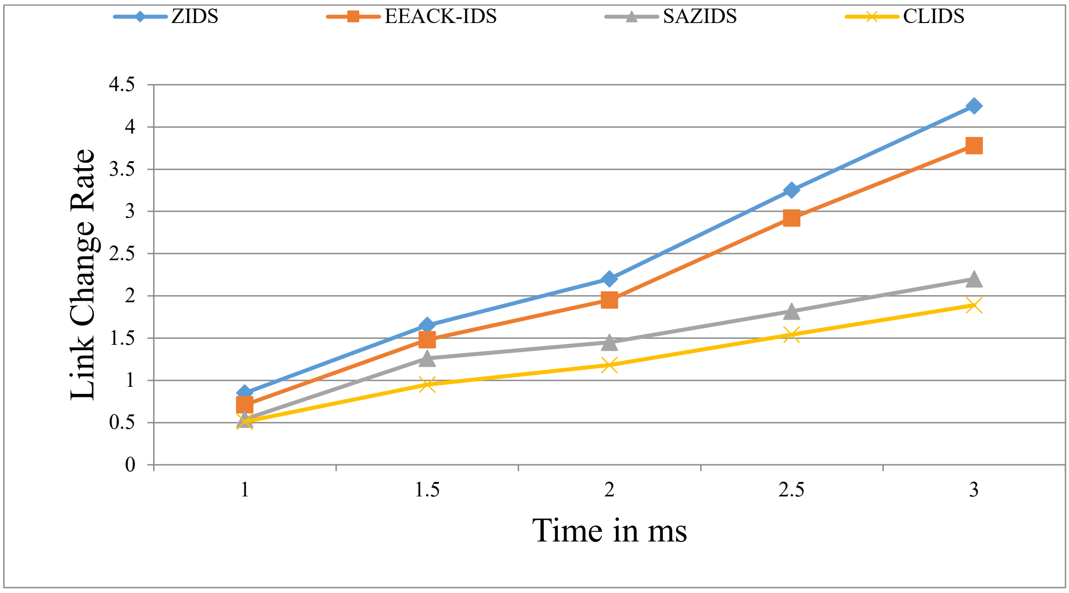

Fig. 5. Link Change Rate Comparison

Mean Time To Alarm

Mean Time to Alarm is shown in Fig. 8. It can be seen that CLIDS can reduce the time to alert compared to the existing technique ZBIDS, EEACK-IDS and SAZIDS. CLIDS shows 11.97% better performance than SAZIDS, 22.89% better than EEACK-IDS, 29.88% enhanced outcome than the current strategy ZBIDS in Fig 6.

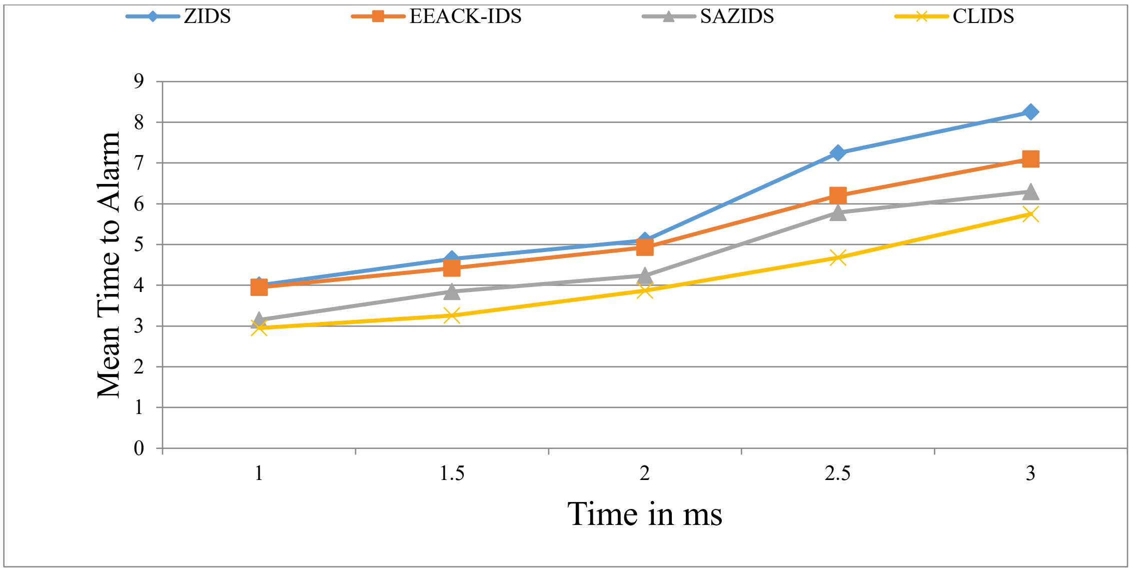

Fig. 6. Mean Time to Alarm Rate Comparison

IV. CONCLUSION

This paper has proposed CLID with the objective of packet dropper identification with considerable energy consumption using cross layer information. The CLID 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 SAZIDS 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.

References

[1]. B. Bains and R. Vaid, "Selective Forwarding based Intrusion Detection System for Secure Wireless Sensor Network," International Journal of Computer Applications, vol. 77, no. 13, pp. 20–26, Sep. 2013.

[2]. G. ZHOU and A. Shrestha, "Efficient Intrusion Detection Scheme based on SVM," Journal of Networks, vol. 8, no. 9, Sep. 2013.

[3]. N. W. Boskany, "Design of Alarm Based Network Intrusion Detection System," Journal of Zankoy Sulaimani - Part A, vol. 16, no. 2, pp. 65–69, Apr. 2014.

[4]. K. V. and S. C. Lingareddy, "A Secure Intrusion Detection System for Heterogeneous Wireless Sensor Networks," International Journal of Computer Applications, vol. 179, no. 1, pp. 1–8, Dec. 2017.

[5]. G. Suseendran and A. Sasikumar, "Secure Intrusion-Detection System in Mobile Adhoc Networks," Indian Journal of Science and Technology, vol. 9, no. 19, May 2016.

[6]. Krishnaveni and M. Ezhilarasi, "Robust intrusion detection system based on fuzzy C means clustering scheme implemented in IoT-based wireless sensor networks," International Journal of Networking and Virtual Organisations, vol. 23, no. 4, p. 312, 2020.

[7]. S. Kamalesh and P. G. Kumar, "Fuzzy Based Secure Intrusion Detection System for Authentication in Wireless Sensor Networks," Journal of Computational and Theoretical Nanoscience, vol. 14, no. 5, pp. 2465–2472, May 2017.

[8]. R. K. Sharma, H. K. Kalita, and B. Issac, "Are machine learning based intrusion detection system always secure? An insight into tampered learning," Journal of Intelligent & Fuzzy Systems, vol. 35, no. 3, pp. 3635–3651, Oct. 2018.

[9]. M. Maheswari and R. A. Karthika, "A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks," Wireless Personal Communications, vol. 118, no. 2, pp. 1535–1557,

[10]. R. Bala Krishnan and N. R. Raajan, "An Enhanced Biometric Based Intrusion Detection System For Secure Communication," Far East Journal of Electronics and Communications, pp. 121–131, Apr. 2016.

[11]. M. P. Arthur and K. Kannan, "Cross-layer based multiclass intrusion detection system for secure multicast communication of MANET in military networks," Wireless Networks, vol. 22, no. 3, pp. 1035–1059, Oct. 2015.

[12]. S. Ponomarev and T. Atkison, "Industrial Control System Network Intrusion Detection by Telemetry Analysis," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 252–260, Mar. 2016.

[13]. T. A., "Hybrid Cuckoo Search Optimization based Tuning Scheme for Deep Neural Network for Intrusion Detection Systems in Cloud Environment," Journal of Research on the Lepidoptera, vol. 51, no. 2, pp. 209–224, Apr. 2020.

[14]. R. Mitchell and I.-R. Chen, "Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, pp. 16–30, Jan. 2015.