Received: August 21, 2017


International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

# Proactive Hybrid Intrusion Prevention System for Mobile Adhoc Networks

**Sharmasth Vali Yerur[1*]** **Prakash Natarajan[1]** **Tiruchirai Ramanujam Rangaswamy[1]**

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

**Abstract:** The open nature of Mobile Ad Hoc NETworks (MANETs) provides an opportunity for intrusions. The current intrusion mechanisms are reactive and incapable of preventing the intrusions proactively. This paper proposes the secure routing using Hybrid intrusion prevention systems against dropping and data integrity THreat (SHEATH). This proposal implements self-key and mutual-key reliant prevention and the appearance frequency based behavior certainty measurement on routing paths. The self-key prevention scheme exploits the encrypted value of the sequence number as a normal pattern and the decryption determine whether the route reply is the result of a malicious node or not. The behavior certainty measurement using distributed selection of Squad Head nodes ensures the effective observation of misuse pattern and minimum routing overhead. The data forwarding phase shares a mutual key between the communicating nodes that prevent the data integrity attacks. The simulation results confirm the efficiency of the hybrid preventive scheme against intrusions.

**Keywords:** MANET, Routing, Packet dropping, Intrusion detection, Intrusion prevention system.

## 1. Introduction

The Mobile Adhoc NETwork (MANET) is an infrastructure-less network, and it is adaptable to numerous potential applications. The MANET is vulnerable to various intrusions due to the open nature of wireless networks. The Intrusion Prevention System (IPS) is an effective way of reacting to the intrusions before the regular routing activities get damaged. The main drawback of Intrusion Detection Systems (IDSs) is that these systems can identify the abnormal behavior of the nodes only after they carry out the damage to the network resources [1] [2]. The anomaly and specification based IDSs audit the data to find out the normal behavior, however, the packet dropping intrusions is most destructive due to its prolonged time consumption for matching the patterns over the period. The primary focus of IDS is to warn the network after it detects suspicious activity. The conventional IDSs techniques are limited because the malicious nodes are capable of capturing and compromising the normal nodes. The malicious nodes snatch the cryptographic keys easily. There are two encryption solutions such as symmetric or asymmetric. In practice, the communicating devices have to share and manage their secret key perfectly. However, once the key has leaked, the IDS fails to prevent the information leakage. Even though IPSs identify the data integrity intrusions, a malicious node can drop the encrypted data packets before identification of the intrusion pattern. The proposed system aims at preventing both the routing and data integrity related intrusions in MANET. The implementation of heavyweight encryption based IPS in MANET seems unaffordable due to the severely constrained node resources. The proposed system depends on the self and mutual-key, and moreover, behavior certainty factor to prevent the data routing from the intrusions of dropping as well as data integrity in MANET. Indeed, the SHEATH implements the light weight prevention system, due to the absence of encryption key sharing and watchdog based IPS implementation on every node. The main contributions of the proposed work are as follows.

- The primary contribution of the work is to propose a secure hybrid prevention system includes self

and mutual key encryption systems and also a trusted measurement to prevent the network, instead of warning the network after a suspicious activity takes place.

- The novel self-key reliant cryptography encrypts the intrusion-target field of the sequence number in route discovery process and decrypts the field using the same key during the route reply process. Using the pattern of the encrypted sequence number, it can identify the presence of a malicious node in a path.
- To identify the collaborative dropping intrusions, the behavior certainty measurement model provides the failure of transmission paths to Squad-Head nodes.
- The distributed Squad-Head takes the measure of node-pair frequency in the suspected paths as a pattern and identifies the collaborative dropping intrusion presence.
- The mutual key reliant encryption model utilizes another disjoint path to share the mutual key and prevents the data integrity intrusions with the reasonable key management overhead.

The remaining part of the paper is organized as follows: Section 2 surveys the previous works related to the intrusion detection and prevention systems. Section 3 describes the system model and proposed methodology with overall functional components. Section 4 analyzes the detection accuracy and the overhead of the proposed intrusion prevention system. Section 5 evaluates the performance of the SHEATH and Section 6 concludes the paper.

## 2. Related work

Several works have been suggested in a MANET to detect and prevent the network from dropping and data integrity intrusions [3]. The intrusion detection systems have been categorized into proactive and reactive mechanisms. The reactive techniques deploy the IPS to take action before the intrusions are launched in the network, whereas the IDS come into action during an intrusion [4]. The IPS provides a unique identity to each user and verifies the credentials of the users to detect the normal pattern. Despite of detecting malicious nodes EAACK [5] identify the misbehaving nodes. EAACK has utilized the DSA algorithm to sign the data packets before transmitting to the destination to cope up with the false misbehavior. In [6], the performance of these classifiers is analyzed to detect malicious activities in MANET. A hybrid IDS (HybIDS) [7] includes cross-correlative detection system and anomaly based intrusion detection. The HybIDS categorizes the nodes as either zero or one. The primary value denotes the suspicious node, and another one is a legitimate node. After the node classification, the second detection engine creates the normal profile using application level interactions. The deviation in the observed interactions from the normal profiles is generated. However, this mechanism suffers from the false positives due to offline training phase. In [8], Worm-hole Avoidance Routing Protocol (WARP) is proposed to prevent the intrusions, especially the wormhole attack. This scheme utilizes the abnormal path attractions to construct the routing table for the nodes in the communication range. The Bayesian game theory based IDS model [9] takes into account the interactions between the players. However, the main drawback in WARP is that it has to maintain the detection accuracy under the dynamic nature of MANETs.

A Mobility and Energy Aware Clustering Algorithm (MEACA)[10] and Intrusion Detection and Adaptive Response mechanism (IDAR) [11] takes into account the node mobility and energy of nodes in cluster formation. The nodes with the same speed and move in the similar direction are grouped to create a static cluster even in the dynamic nature of MANETs. However, the actual performance of MEACA is uncertain due to the single point of failure. In [11], a cryptographic based distributed IDS is proposed for fault tolerance. This technique exploits leader and collector nodes. The leader nodes involve in high-level functions, whereas the collector nodes perform low-level functions for IDS. However, the performance of the system decreases with the severity of malicious environment, due to the packet loss induced by high routing overhead. To detect the black-hole attacks, a novel approach [12] named as Anti-Black-hole Mechanism (ABM) is proposed. All the nodes set the IDS nodes in promiscuous mode to detect malicious nodes before launching the intrusions. According to the abnormal difference between the processes of route discovery and reply, the suspicious value of the neighboring nodes is updated in a table. If the suspicious value exceeds the threshold value, the node is considered as a black-hole intruder. Moreover, the IDS promptly generate alarm against the malicious nodes.

A host-based Intrusion Detection technique using Anomaly Detection (IDAD) [13] is used to prevent the black hole attacks. The detection mechanism monitors the network activities and differentiates the malicious activities from the traffic using a pre-collected set of anomaly activities. If the profile matches, the malicious node is isolated from the network immediately. However, the false

negative rates are increased with the variants of black-hole intrusions in the MANET. Moreover, the memory utilization of IDAD technique is high, due to the maintenance of four different routing tables in every node. It reduces the speed of IDS and detection accuracy. In [14], the Intrusion Detection and Adaptive Response (IDAR) mechanism has proposed. By taking into account the network characteristic information, the IDAR identifies the variants of dropping attacks, sleep deprivation, and rushing attacks successfully. Even though, the usage of clustered MANET improves the security of system, the escalation of routing overhead is not considered. In addition, the response system punishes the attackers adaptively according to the impact of attackers on the network performance. The IDAR selects a longest path around the attackers tends to high delay, especially in a highly vulnerable environment. The same issue of IDAD system has not been handled in [15] also. The distributed watchdog implementation reduces the routing overhead and improves the routing performance even in the presence of mobility in the network. However, the improper selection of an optimal number of watchdog nodes and distance among them may tend the system to underutilize the advantages of IDSs. The encryption based IDSs do not assure the security of MANET against black-hole, gray hole attacks, and sequence number based routing attacks. Thus, there is a need for presenting a hybrid defense system without increasing the routing overhead and communication delay.

## 3. Overview of the proposed methodology

Designing an IPS which is capable of preventing the network against both the dropping and data integrity relevant intrusions is a challenging task. The reason is that despite several IPSs have been built for every integrity intrusion using encryption and authentication techniques, their implementation seems too expensive for packet dropping intrusions. Due to the severely constrained network resources, building the centralized IPS model is not suitable for MANETs. The primary objective of this work is to design a scalable and low-complexity IPS to avoid malicious nodes issuing routing and integrity related intrusions. The proposed SHEATH system introduces the Self-Key Reliant Route Discovery and the Appearance frequency of a node pair in malicious paths to detect individual and cooperative dropping intrusions respectively. The proposed SHEATH utilizes the mutual key reliant data forwarding in the shortest path, in which the source and destination share a common key via the next shortest path. Thus, the implementation of SHEATH in MANET ensures the protection against both the dropping and integrity intrusions successfully.

### 3.1 System model

Consider the multi-hop MANET as a graph $G = (V, E)$, where $V$ denotes a set of nodes $(N)$ that are distributed in the network and E symbolizes a set of direct edges. Each $E$, i.e., a $\forall$ pair of $N \epsilon V$ makes bi-directional communications. It means that the node $A \epsilon V$ is in the transmission range ($R_B$) of node B $\epsilon$ V and vice versa. The direct connection $(A, B) \in E$ represents that the node B is located within R of node A. Node B is an active neighboring node of A, $B \in AN_B$. The source node $N_s$ initiates the route discovery process to the destination $N_d$, by broadcasting the RREQ packets with Sequence Number ($SN$) and Hop Count ($HC$).

$$AN_{A<-B} = (A,B) \in E^{\wedge} (B \in N) \quad (1)$$

The high value of SN represents the freshness of a route, and the HC represents the number of hops to reach the $N_d$. The destination node $N_d$ replies the $N_s$ through Multiple node disjoint routes $Ro, (Ro \in \{N_s\text{-}Nr_1\text{-}Nr_2\text{-}....Nr_{i-1},N_d\}, \{Ns\text{-}Nr_i\text{-}Nr_{i+1}\text{-}....Nr_n,N_d\},.....Ns\text{-}Nr_{n+1}\text{-}Nr_{n+2}\ldots\ldots\ldots\ldots Nr_{n+n},N_d\})$. According to the $SN$ and $HC$, the $N_s$ selects the path for data routing.

#### 3.1.1. Malicious scenario

The active intrusions involve in communication data dropping, modification, or fabrication to disrupt the normal functionality of routing protocol in MANET. In MANET, a dropping intruder launches different intrusions in the following ways. It is likely to change the factors in the route reply packet such as a sequence number and hop count. In packet drop intrusion such as black, gray, and so on. Malicious node stops to rebroadcast the route request packet and generates the fake route reply with lowest HC and highest SN to act as one of the intermediate nodes in a route. As per the routing protocol, the Ns select a malicious path, and an intruder drops all the received packets. An individual harmful node uses the route reply method to self-claim that it has the shortest path to the destination node, but it does not collaborate with others are placed nearby. In contrast, the collaborative intruders launch intrusion together to beguile the legitimate nodes. Unlike malicious data dropping, in data integrity relevant intrusions, an intruder node changes the contexts of messages sent by legitimate nodes and misleads them from knowing the original data.

#### 3.1.2. Intrusion prevention system

Every node generates a self-key ($S_{key}$) periodically, and this key is used to route discovery that is free from the individual dropping intrusion, especially those intrusions are launched using the factors of *SN* and *HC*. Every node broadcasts the route request packet with the original and the encrypted field of the self-key using SN. When the same node receives the route reply packet, it decrypts the particular field using the SN in the reply packet. If the same self-key value is retrieved, the node routes the reply packet to the sender node. Otherwise, it sends an alert packet to the Squad-Head node. In the case of collaborative intruders, the sender node receives fewer ack packets through a path using behavior certainty measurement, and the IPS informs an entire path as suspected through overhearing. The distributed selection of Squad-Head nodes initially divides each region into k number of Sectors to select only a limited number of trusted nodes as head nodes (Hds) $\epsilon$ N. The Hds are responsible for confirming the individual and collaborative dropping intrusions in a path using the appearance frequency of a node pair in suspected paths. Moreover, the sender node shares a random number with the destination through another shortest path. By using the random number, the source and destination estimate the Mutual key ($M_{key}$) for secure communication. After verifying the entire path, the sender node starts to send the original encrypted data packets to the destination using $M_{key}$.

### 3.2 Hybrid IPS in route discovery process

The trust measure alone is not enough to prevent the network against dropping intrusions since it relies on cooperative behavior during route discovery. The secure key used for encryption needs to be the main consideration during the design of IPS to prevent the MANET against intrusions. However, if the dropping node has dropped the encrypted packets during routing, the encryption technique is not that much helpful. Thus, the implementation of IPS in the route discovery process is crucial to prevent the network against intrusions. Mostly, the dropping intrusions reply the source node with the modified features of the sequence number by pretending to be a neighbor of the destination node to get the data. To do this, the SHEATH introduces the self-key reliant cryptography in the route discovery process.

#### 3.2.1. Intrusion detection using self-key reliant cryptography

Like symmetric encryption, every node in the network generates a unique self-key $S_{key}$ individually. Conventionally, the data can be encrypted by the key to ensuring data privacy. In contrast, the data privacy is not a goal of self-key reliant cryptography. However, the objective of SHEATH is to identify the modification of SN during the route reply phase. Generically, it is forced to store the sequence number of every request packet in a node memory to ensure the modification. To avoid this additional storage requirement, instead of encrypting the entire packet, only the dropping intrusion target field is encrypted. The target file of most of the dropping intrusions is a sequence number.

During the route discovery process, every receiver applies the self-key reliant cryptography i.e. Encrypting the $S_{key}$ with SN number. By using the common and pre-stored key value, the receiver behind the RREP packet originator can easily verify the misbehavior of a corresponding RREP sender without storing the SN value for every RREQ process. The packet sender applies the self-key reliant cryptography and attaches the encrypted field in a packet in addition to original SN.

The intermediate receiver again encrypts its self-key with encrypted SN and drops the previous encrypted field of the packet. Every packet receiver repeats this process. The node which is a route to the destination, generating the route reply packet with last received the encrypted packet. The previous hop to the RREP originator verifies the SN value to identify whether it is a dropping intrusion or not. If it is not the intruder, others just forward the reply packet to the sender node without decrypting the packet header. The Eq. (2) shows the encryption of $S_{key}$ using SN value.

$$New_{SN} = enc\ SN\left(S_{key}\right) \tag{2}$$

Consider a scenario, where the Route REQuest (RREQ) packet is flooded into the network by *Ns* towards *Nd*. Initially, the node *Ns* selects the *SN* value and encrypts the self-key a by *SN (E-SN)*. It appends the *SN* and *E-SN* in the packet header before flooding the packets into the network. Every RREQ receiver applies this cryptography using its own $S_{key}$. A black-hole intruder *M* that receives the RREQ packet replies the *Ns* with highest *E-SN3*. When a legitimate previous node *C* receives the Route REPly (RREP) packet, it applies decryption using the *E-SN2* and *E-SN3* which are attached to the received RREP packet. If the decrypted value is

equal to the $S_{key}$ of node C (i.e. a3), the node *M* is a legitimate node which is unable to change the *SN* to a high value. Otherwise, it is an intruder, and the node *C* creates an alert message against node *M*. Moreover, the corresponding RREP packet is not processed further by node *C*. In case, the node *M* is not a malicious or the decrypted value is equal to the *a3*, the previous intermediate nodes towards the $N_s$ do not apply the decryption process during RREP forwarding. Moreover, no need to execute the self-key decryption process, when the destination creates the RREP packet. This process can successfully identify the individual dropping intrusion.

### 3.3 Distributed squad head based collaborative intrusion detection

The proposed self-key reliant cryptography is going to fail when the collaborating dropper plan not to reveal the changes of SN value by the malicious router to the network and replies the sender node with correct SN value. Although the SN value does not change in the RREP packet, the Ns may select the malicious path due to the smallest hop count which is attached to the malicious router. The collaborative intrusion is quite dangerous to the routing performance. To remedy this problem, the SHEATH applies appearance frequency based collaborative intrusion detection on test data forwarding over time. Due to the usage of self-key reliant cryptography along with the appearance frequency based collaborative intrusion detection, the SHEATH is named as hybrid IPS against the individual and collaborative routing intrusions. For implementing the appearance frequency based collaborative intrusion detection, the SHEATH selects the distributed Squad head nodes in the network and enables the test forwarding scenario, before initiating the original data forwarding.

#### 3.3.1. Selection and rotation of distributed squad heads

The SHEATH randomly selects '*n*' number of nodes as Squad head nodes to perform the appearance frequency based collaborative intrusion detection. The Squad head collects the behavior certainty value of a path from the test forwarding scenario and executes the fusion process for collaborative intrusion detection. According to the network area and node transmission range R, the number of Squad head '*Hd'* is decided. The *H* and *W* denote the network height and width respectively. The following equation ensures the selection of '*Hd'* with the distance of minimum *k* hops.

$$|Hd| = \frac{(H \times W)}{(k \times \pi \times R^2)} \quad (3)$$

The IPS in selected Squad head nodes advertises the control message to notice its leadership with k-hop TTL value. A node which is associated with the Squad head sends the response message to the selected head. If any *Hd* does not receive a control packet, it selects itself as a Squad head and continues to flood the advertisement message with k-hop TTL value. The *Hd* provides its leadership role to the neighboring *Hd*, and it returns to the normal state when a *Hd* receives a less number of response messages from the k-hop neighboring nodes. The nodes update its behavior certainty value of its corresponding Squad head. The use of Squad head supports to identify the behavior certainty of a path, before initiating the original data forwarding. The Squad head nodes share their uncertain node pairs to a neighbor node when it moves to another location. Then, the selected new Squad head announces its ID as *Hd* to the nodes around k-hops using control packets. Thus, the Squad head can successfully identify the correlated node pairs from the suspected routing paths using a test forwarding scenario.

#### 3.3.2. Collaborative intrusion detection using squad-head

After receiving the RREP packet either from the destination or the intermediate router, the SHEATH enables the test forwarding scenario to measure the behavior certainty level of a path. The collaborative intruders may find their location in the selected routing path. In the test scenario, the $N_s$ sends the encrypted dummy data packets to the destination. When the destination node $N_d$ receives a data packet, it adds the ID of successfully received packets in a list *L*. After t time; the destination sends the list *L* to the $N_s$ via another route because it is possible that the malicious nodes located in a test path may drop the acknowledgment packet. On the arrival of the packet, the source node $N_s$ extracts the number of received packets $=\{p_1, p_2, \ldots p_n\}$, where $p_i$ refers to the identity of a packet. If the value of $|p|$ is closer to the number of sending packets, the selected path is called a normal path. Otherwise, the path is informed as suspected to the corresponding *Hd* of source node $N_s$. Every *head* node executes the appearance frequency based collaborative intrusion detection periodicals. Considering $X = \{X_1, X_2, .. X_n\}$ and $X_n$ is the number of suspected paths that are announced by the neighboring nodes. The path length of $X_i$ is $PL_i$. The number of node pairs ($N_{ij}$) appears in the suspected pathshare $PL_i$-*1*. Where *A* is

an input node pair, $N_{ij}$ and the Eq. (4) returns the result of the number of frequency of node pair in suspected paths. The behavior certainty value of every path is informed to the corresponding source node by the *Hd*. In this way, the SHEATH performs intrusion prevention by analyzing the malicious link in suspected paths. According to the behavior certainty value of $path_i$, the source decides the data forwarding path.

$$Behavior\ Uncertainty\ (A) = \sum(N_{ij} \cap A) \quad (4)$$

$$Behavior\ Ceratinty(Path_i) = \begin{cases} 0 & if\ any\ A \in PL_i > threshold \\ 1 & otherwise \end{cases} \quad (5)$$

If it is not trustworthy, the source selects the second shortest path for a test case, and notably, the second path excludes the identified uncertain links. Moreover, this scheme ensures the trustworthiness of a path for data forwarding. However, there remains another issue of data integrity intrusions. Both the implementation of self-key reliant cryptography and appearance frequency based intrusion detection is not efficient to cope up with the data modification and integrity intrusions.

### 3.4 Mutual key reliant data encryption

To cope up with the data integrity intrusions, the proposed SHEATH takes into account the mutual key reliant data encryption. This scheme handles the privacy and security intrusions between the communicating nodes in the network. The mutual key reliant data forwarding that includes key searching and mutual key updating and prevents tracing, impersonation, and overhearing intrusions. When the communicating nodes demand wireless communication, those nodes need to agree on a secret key between them. Every time a source node sends an encrypted packet using the mutual key and the destination node that receives the message decrypt the encrypted message using the same key. The steps involved in the mutual key reliant data forwarding are as follows.

- The source node starts to broadcast the RREQ packets with encrypted *SN*, original *SN*, and destination ID.
- The destination or any intermediate router that has a route to the destination replies the source node via the reverseroute.
- Likewise, the source node may receive more than one RREP via disjoint routes from the destination.
- Initially, the source node selects the second shortest path and sends a secret key $K_{i,integ}$ to the destination.
- Then, the destination generates a Random Number (RN) and sends the encrypted RN by $K_i$ when it receives $K_{i,integ}$ from the source.
- This information is sent via the shortest path between the source and destination. $Ki_{integ}$ decrypts the encrypted random number *RN*, to produce the RN value to the sender node.
- After that, the sender node starts its secure data transmission followed by the test forwarding.

Without knowing the mutual key ($M_{key}$), the integrity intrusions fail to launch the data integrity intrusions. The storage and overhead cost of mutual-key sharing is not much high as symmetric and asymmetric cryptography techniques. Thus, the proposed SHEATH provides an effective prevention system against the data integrity intrusions.

## 4. Security analysis of SHEATH

The idea of exploiting hybrid IPS is appealing in wireless network security because it can detect intruders with different purposes such as dropping. However, an escalated routing overhead refuses to utilize the advantage of the IPS, and it increases the number of failed transmissions in MANET. Thus, the proposed SHEATH including self-key reliant secure route discovery and mutual-key reliant data forwarding increases the intrusion detection and network throughput significantly. The following section formulates the performance of the proposed SHEATH in terms of detection accuracy, throughput, and overhead.

Let *X* and *Y* be defined as the detection accuracy and the routing overhead. In SHEATH, *X* is the average of detection accuracy of individual dropping, collaborative dropping, and data integrity.The changed *SN* value by the individual droppers is successfully identified by the legitimate previous hop in the same path. However, during the test forwarding scenario, the data packets or the acknowledgment packets for the successfully received data packets may lose at the legitimate node due to network collision. This reduces the intrusion detection accuracy. Where the $\lambda$ denotes the number of packet droppers due to the collision, but misclassified as dropping intruders.

$$x_{dropping} = 1 - \left(\lambda / Total\ number\ of\ nodes\right) \quad (6)$$

Due to the selection of disjoint paths during the mutual key sharing, the detection accuracy of data integrity is not reduced significantly. In the case of

low traffic, there is a possibility for overhearing the mutualkey sharing.

The average of $x_{dropping}$ and $x_{integrity}$ is the detection accuracy of SHEATH protocol. The value of detection accuracy $X$ is shown in Eq. (8). Moreover, the routing overhead is not much higher as found in the symmetric and asymmetric cryptography techniques. For instance, when considering in the symmetric encryption, all the nodes have a secure key.

$$x_{integrity} = 1 - \left\{ \begin{matrix} \text{Number of} \\ \textit{Busy} \text{ links} \end{matrix} \Big/ \begin{matrix} \textit{total} \text{ number of} \\ \textit{integrity} \text{ Intruders} \end{matrix} \right\} \quad (7)$$

$$X = {}^{1}\!/_{2} \times \{x_{dropping} + x_{integrity}\} \quad (8)$$

For every transmission, the sender node needs to share the key with the destination using external key sharing techniques. This key sharing increases the control overhead drastically. However, the routing overhead of SHEATH is as shown in Eq. (9).

$$Y = Routing\ Protocol_{Overhead} + (k \times N) + (Hop\ count \times t/data\ interval) \quad (9)$$

The value of *Routing Protocol* $_{Overhead}$ is equal to the overhead in AODV and $(k \times N)$ represents the routing overhead induced by the Squad Head selection process. Moreover, the last term in the Eq. (8) denotes the consideration of all the test data packets for appearance frequency based intrusion detection as control overhead.

## 5. Performance evaluation

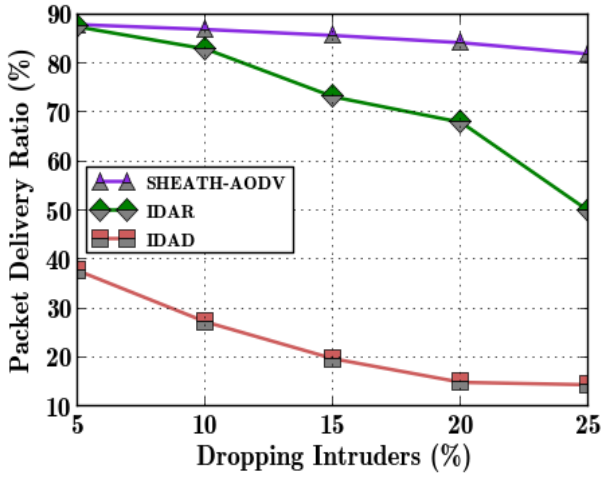
The proposed SHEATH-AODV is compared with the existing IDAD [13] and IDAR [14]. The performance is evaluated over a randomly distributed of mobile nodes, and it is set to 50. The nodes move with the speed of 5m/s over an area of 1000m x 1000m. The communication range of nodes is 250m. The SHEATH follows Constant Bit Rate (CBR) and User Datagram Protocol (UDP) in the application and the transport layer respectively. This scenario enables six CBR connections with the packet size of 1024 bytes, and the packet transmission interval is 0.1s. The network bandwidth is 2 Mbps and the total simulation time is 100s. To compare the performance of SHEATH-AODV, IDAD, and IDAR, the number of dropping intruders is varied from 5% to 25%. This scenario creates low to high threat environment. Moreover, to evaluate the performance of SHEATH-AODV over various traffic rate, the number of data flow is varied from 2 to 10 number of source-destination pairs.

### 5.1 Simulation results

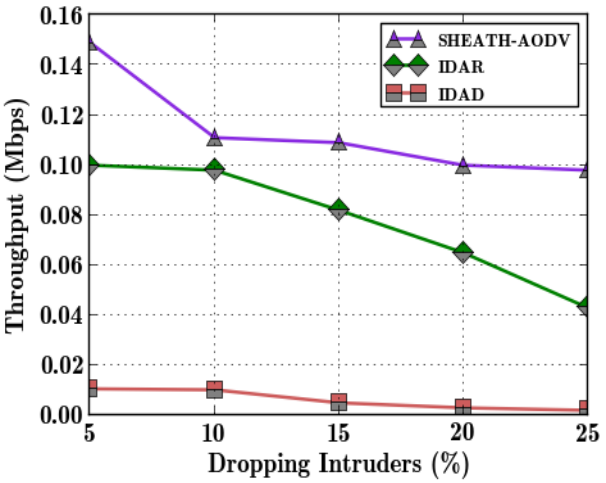
The number of malicious nodes and data flows are varied to illustrate the performance of the proposed SHEATH-AODV protocol.

#### 5.1.1. Dropping intruders vs. packet delivery ratio and throughput

The performance of SHEATH-AODV, IDAR, and IDAD is compared by varying the dropping intruders from 5 to 25% over 100 node topology, as shown in Fig. 1. When the number of dropping intruders is less, the packet delivery ratio of SHEATH-AODV and IDAR approach nearly 90%. The IDAD fails to determine the variability of dropping intruders that lead to a poor packet delivery ratio. Even at high threat environment, the SHEATH-AODV delivers the packets as expected.

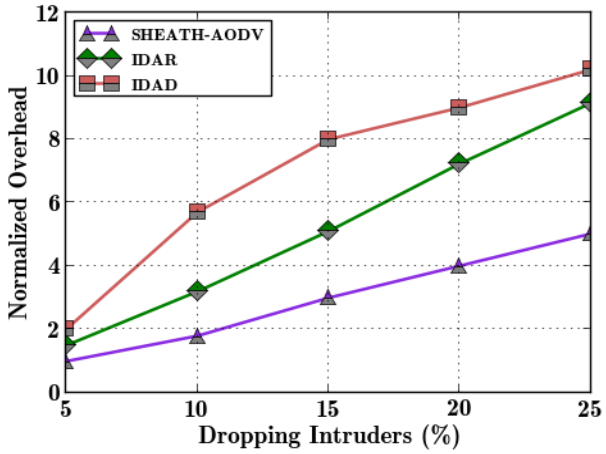



(a)

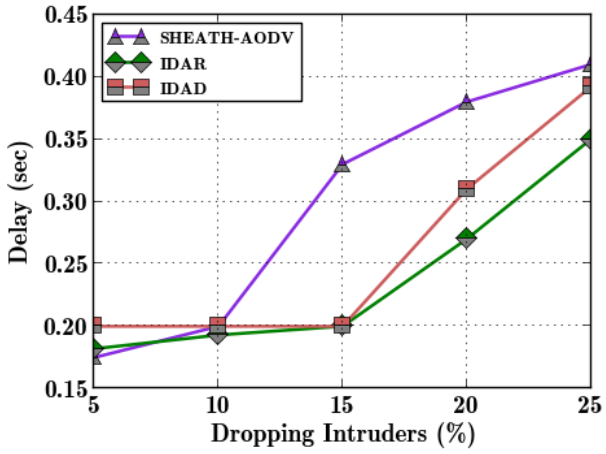



(b)

Figure.1 Dropping intruders vs. packet delivery ratio and throughput




(a)




(b)

Figure.2 Dropping intruders vs. normalized overhead and delay

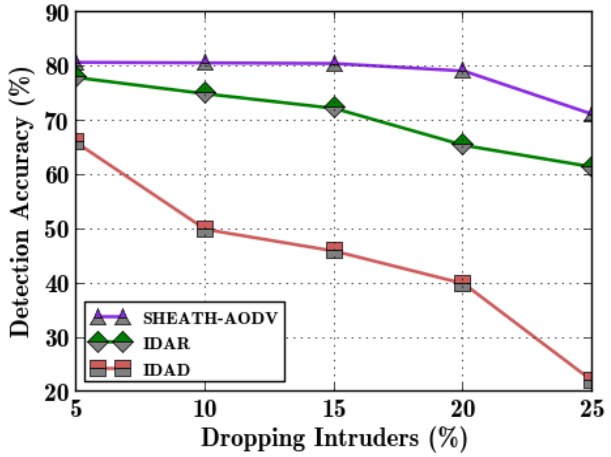



Figure.3 Dropping intruders vs. detection accuracy

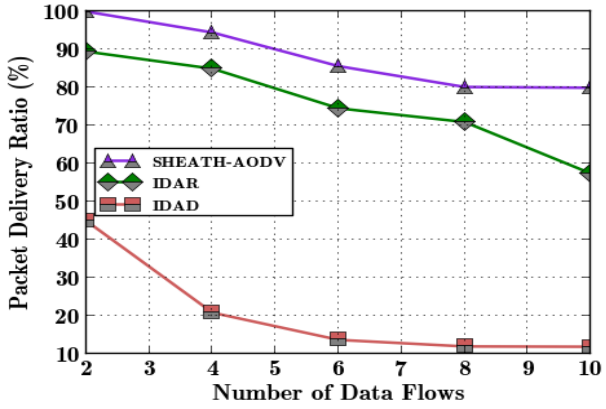
The reason behind is that the elimination of both individual and collaborative intruders using the hybrid prevention system. The SHEATH-AODV drops the PDR from 89% to 82% when the number of drop-in intruders increases as shown in Fig. 1 (a). However, IDAR drops the PDR from 89% to 50% when the number of drop-in intruders increases. The PDR difference is significant in the high threat environment with the presence of 10 to 25% intruders since the collaborative intruders can easily break the anomalous pattern-based detection scheme. The Fig. 1 (b) illustrates that SHEATH-AODV attains better throughput than IDAR and IDAD obviously. For example, the throughput of SHEATH-AODV drops from 0.15 to about 0.10 Mbps with increased percentage of dropping intruders whereas the IDAR and IDAD have fallen from 0.10 to 0.04 Mbps and from 0.01 to 0.00084 Mbps respectively.

#### 5.1.2. Dropping intruders vs. overhead and delay

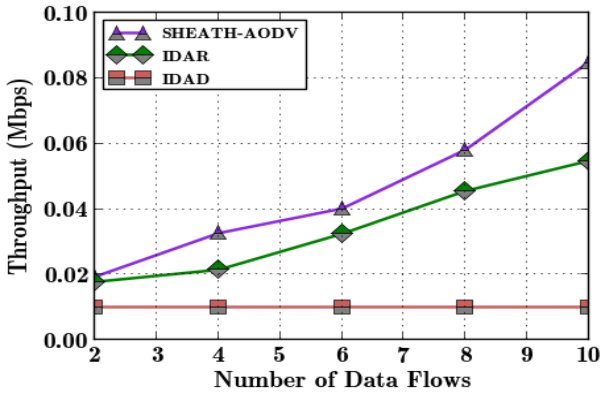
Fig. 2 shows the performance results of SHEATH-AODV, IDAR, and IDAD when changing the number of dropping intruders. When the percentage of packet dropping intruders increases to 25%, the overhead of SHEATH-AODV, IDAR, and IDAD are approximately 5, 9, and 10.1% respectively as shown in Fig. 2 (a). The IDAR increases the routing overhead due to the clustered network topology and increased time to live of route request packets. Even though, the IDAD is an intrusion prevention system, the performance of IDAR is better than the IDAD. However, the IDAR includes the network characteristics to identify the dropping intruders accurately. It sharply escalates the routing overhead more than the mutual key sharing concept in SHEATH-AODV. In low threat environment, the delay in SHEATH-AODV is lower than that of IDAR and IDAD. The reduced delay in SHEATH-AODV is primarily due to the path verification using Squad-Head nodes. The IDAR selects a longest path around the intruders and IDAD frequently determines the routing path, due to improper intrusion detection. When the intruders are 5%, the delay of SHEATH-AODV is low, whereas in 10% of attackers the delay of SHEATH-AODV, IDAR, and IDAD are approximately 0.20 seconds. Beyond the 10% of intruders, the SHEATH-AODV exhibits a high delay compared to the IDAR and IDAD.

#### 5.1.3. Dropping intruders vs. detection accuracy

In Fig. 3, the intrusion detection accuracy is high in SHEATH-AODV compared to the IDAR and IDAD, due to the usage of hybrid prevention systems in the proposed work. The self-key encryption scheme of SHEATH-AODV in the route discovery process shows the malicious activities in the network earlier and prevents the network successfully. On the other hand, the matching of anomaly patterns in IDAD takes more time since the

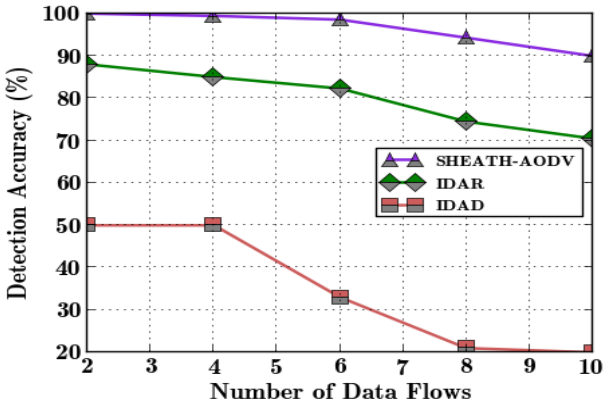



(a)

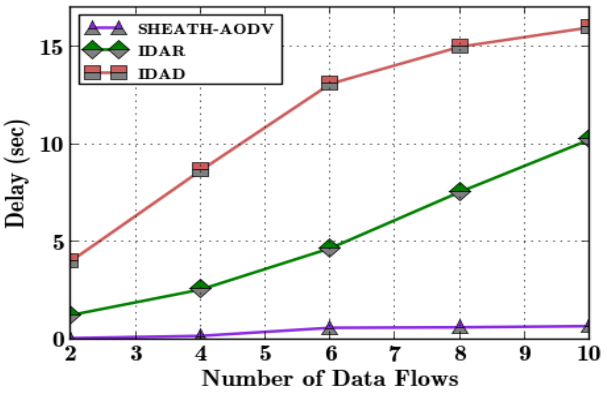



(b)

Figure.4 Number of data flows vs. packet delivery ratio and throughput




(a)




(b)

Figure.5 Number of data flows vs. delay and detection accuracy

impact of dropping intruders on the selected path exists, this increases the detection time gets extended, resulting in reduced accuracy of IPS in IDAD.

Compared to IDAD, the IDAR increases the detection accuracy, due to the consideration of network characteristics. For instance, in Fig. 3, the SHEATH-AODV, IDAR, and IDAD attain detection accuracy of 70%, 62%, and 22% respectively under high vulnerable environment. In addition to the individual intruder detection, the distributed usage of Squad-Head nodes supports the SHEATH-AODV to improve the detection accuracy over a collaborative threat environment.

#### 5.1.4. Number of data flows vs. packet delivery ratio and throughput

Fig. 4 shows the performance results of SHEATH-AODV, IDAR, and IDAD by varying the number of data flows from 2 to 10 with 15% of intruders in the environment. From the Fig. 4 (a) and 4(b), it is observed that the high traffic creates a high impact on the IDAR and IDAD. A huge number of data packets increase the impact of the collision on intruder detection and reduce the packet delivery ratio of SHEATH-AODV. From the Fig. 4 (a), the packet delivery ratio of SHEATH-AODV reduces by 20% while increasing the number of data flows, due to the lack of considering network collision dropping into account.

Both the IDAR and IDAD drop the packet delivery ratio by more than 25% from low to high threat environment since the assumption of IDAR and IDAD is that a node ID cannot be forged and the threshold for a malicious activity is pre-defined respectively. This is the main reason why that the packet delivery ratio in IDAR and IDAD is less. However, the throughput of SHEATH-AODV increases by 76.4% with the data traffic, as shown in Fig. 4 (b).

#### 5.1.5. Number of data flows vs. delay and detection accuracy

Fig. 5 shows the comparative performance of SHEATH-AODV, IDAR, and IDAD by varying the number of data flows from 2 to 10. The SHEATH-AODV observes the normal pattern of a node in route discovery phase, and it also takes the support of Squad-node decision to detect the intruders. This technique increases the detection accuracy of SHEATH-AODV and shortens the packet delivery delay in the network. For instance, in Fig. 5 (b), the

SHEATH-AODV, IDAR, and IDAD deliver the data packets in 0.02 Sec, 1 Sec, and 4 Sec respectively. In the Fig. 5 (a), the detection accuracy of SHEATH-AODV in various data flows degrades linearly due to the accumulation of packet loss caused by the collision as the Squad Head nodes may incorrectly select the packet loss due to the collision as malicious activity. Due to the usage of hybrid prevention systems, the detection time of SHEATH-AODV is always lesser than that of IDAR and IDAD. It reduces the impact of packet dropping on malicious pattern mapping in SHEATH-AODV and improves the detection accuracy. For instance, in Fig. 5 (a), with high numbers of data flows the SHEATH-AODV, IDAR, and IDAD attain a detection accuracy of 90%, 70%, and 10% respectively.

## 6. Conclusion

This work has presented a hybrid prevention system against dropping and data integrity intruders in MANET. The proposed SHEATH considered the self-key and distributed Squad-Node decision in differentiating the normal patterns from the intrusion patterns. It has demonstrated the efficient packet delivery capability of SHEATH-AODV in the presence of 5%-25% of dropping intruders in MANET. Finally, the performance is evaluated for the extended SHEATH-AODV by varying the percentage of intruders and number of data flows. The evaluation of SHEATH-AODV protocol shows the improved detection accuracy of the hybrid IPS by nearly 10% and 48% in MANET, compared to the existing IDAR and IDAD respectively. There are several possible directions for the proposed work to extend in the future, and those directions are summarized as follows. In future, the identification of unknown intrusions needs to be considered in the design of intrusion prevention system. Moreover, to avoid the impact of node mobility on the detection accuracy of IPS, it is essential to integrate the mobility of nodes into account to discover a highly secure routing path.

## References

[1] S. Kumar and K. Dutta, “Security issues in mobile ad hoc networks: A survey”, *Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications*, pp.176-221, 2014.

[2] T. Anantvalee and J. Wu, “A survey on intrusion detection in mobile ad hoc networks”, *Wireless Network Security,* Springer US, pp. 159–180, 2007.

[3] S. Kumar and K. Dutta, “Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges”, *Security and Communication Networks*, Vol.9, No.14, pp.2484-2556, 2016.

[4] A. Nadeem and M. Howarth, “A survey of MANET intrusion detection & prevention approaches for network layer attacks”, *Communications Surveys & Tutorials IEEE*, Vol. 15, No. 4, pp. 2027-45, 2013.

[5] E. Shakshuki, N. Kang, and T.R. Sheltami, “EAACK-a secure intrusion-detection system for MANETs” *Industrial Electronics, IEEE Transactions*, Vol. 60, No.3, pp. 1089-1098, 2013.

[6] S. Pastrana, A. Mitrokotsa, A. Orfila and P. Peris-Lopez, “Evaluation of classification algorithms for intrusion detection in MANETs”, *Knowledge-Based Systems*, Vol.36, pp.217–225, 2012.

[7] A. Lauf, R.A. Peters, and W.H. Robinson, “A distributed intrusion detection system for resource-constrained devices in ad-hoc networks”, *Ad Hoc Networks*, Vol. 8, No.3, pp.253–266, 2010.

[8] M.Y. Su. “WARP: a wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks”, *Computers & Security*, Vol. 29, No.2, pp.208–224, 2010.

[9] H. Wei and H.S. Wei, “Using bayesian game model for intrusion detection in wireless ad hoc networks”, *International Journal of Communications, Network & System Sciences*, Vol. 3, No.7, pp.602–607, 2010.

[10] E. Darra, C. Ntantogian, C. Xenakis, and S. Katsika, “A mobility and energy-aware hierarchical intrusion detection system for mobile ad hoc networks”, In: *Proc. of the International conference on Trust, Privacy and Security in Digital Business*, Springer: Berlin/Heidelberg, pp.138–149, 2011.

[11] P.M. Mafra, J. Fraga, and A.O. Santin, “Algorithms for a distributed IDS in MANETs”, *Journal of Computer and System Sciences*, Vol. 80, No.3, pp.554–570, 2014.

[12] M.Y. Su, “Deployment of intrusion detection nodes to prevent wormhole attacks in mobile ad hoc networks”, *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 7, No.4, pp.246–260, 2011.

[13] Y.J. Alem and Z.C. Xuan, “Preventing black hole attack in mobile ad-hoc networks using anomaly detection”, In: *Proc. of the 2nd IEEE International Conference on Future Computer*

*and Communication*, Wuhan, China, Vol.3, pp.672–676, 2010.
[14] A. Nadeem and M. Howarth, "An intrusion detection & adaptive response mechanism for MANETs", *Ad Hoc Networks*, Vol. 13, pp.368–380, 2014.
[15] A. Nadeem and M. Howarth, "Protection of MANETs from a range of attacks using an intrusion detection and prevention system", *Telecommunication Systems Journal, Springer*, Vol. 52, pp.2047-2058, 2013.