J Electr Eng Technol.2018; 13(5): 2086-2098
http://doi.org/10.5370/JEET.2018.13.5.2086

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

Unethical Network Attack Detection and Prevention using Fuzzy based Decision System in Mobile Ad-hoc Networks

R. Thanuja† and A.Umamakeswari*

Abstract – Security plays a vital role and is the key challenge in Mobile Ad-hoc Networks (MANET). Infrastructure-less nature of MANET makes it arduous to envisage the genre of topology. Due to its inexhaustible access, information disseminated by roaming nodes to other nodes is susceptible to many hazardous attacks. Intrusion Detection and Prevention System (IDPS) is undoubtedly a defense structure to address threats in MANET. Many IDPS methods have been developed to ascertain the exceptional behavior in these networks. Key issue in such IDPS is lack of fast self-organized learning engine that facilitates comprehensive situation awareness for optimum decision making. Proposed "Intelligent Behavioral Hybridized Intrusion Detection and Prevention System (IBH_IDPS)" is built with computational intelligence to detect complex multistage attacks making the system robust and reliable. The System comprises of an Intelligent Client Agent and a Smart Server empowered with fuzzy inference rule-based service engine to ensure confidentiality and integrity of network. Distributed Intelligent Client Agents incorporated with centralized Smart Server makes it capable of analyzing and categorizing unethical incidents appropriately through unsupervised learning mechanism. Experimental analysis proves the proposed model is highly attack resistant, reliable and secure on devices and shows promising gains with assured delivery ratio, low end-to-end delay compared to existing approach.

Keywords: MANET, Intrusion detection and prevention system, Intelligent client agent, Smart server, Fuzzy inference, IBH_IDPS.

1. Introduction

Mobile Ad-hoc Networks (MANETs) represents an autonomous system of movable nodes to form an infrastructure-less, self-organizing, and rapidly deployable wireless network. In recent years, the use of MANETs has been widespread and highly appealing to a lot of applications such as disaster relief, space communication, mission critical battlefield communication etc., For example, in military operation, it serves to provide voice and data communication amongst roaming entities like military personnel's, vehicles, information head quarters etc. Attack recognition and event dissemination in Tactical MANET environment is the focus of this work. Due to its wide open and dynamic characteristic, detecting attacks [1] in a tactical mobile ad-hoc network is a daunting task.

Usage of peer-to-peer wireless ad-hoc networks by the army in the battlefield arena imparts multitude of vulnerabilities and prove to be detrimental to the users. MANET suffers from all-weather attacks, which can come from any node that is in the radio range with any other node in the network. The attacks mainly include passive eaves dropping, leakage of secret information, gray hole, black hole, worm hole, denial of service etc.

Unique characteristics and open nature of Tactical MANET has attracted new security threats, while security aspects in military applications have been rarely addressed. Primary objective of this work is to overcome the difficulties in current Tactical MANET environment. Aim is to develop an inference and correlation specific behavioral based intrusion detection and prevention system to detect complex multistage attacks where fixed relationship is unattainable. Significant effort on research resulted in implementing an "Intelligent Behavioral Hybridized Intrusion Detection and Prevention System (IBH_IDPS)" capable of detecting and preventing attacks in tactical MANET with data delivery accuracy approaching 99%. The IBH_IDP System primarily constitutes the following:

- a knowledge-base (set of if-then rules);
- a working memory or database of derived facts; and
- an inference engine containing the reasoning logic used to process the knowledge base.

In addition, it comprises of distributed virtual head nodes [2-5] (also referred as Intelligent Client Agent (ICA)) used as a decision processing unit connected to a centralized Smart Server (SS) that incorporates fuzzy inference [6-9] based decision making unit. The fuzzy inference engine essentially is a rule-based processing

† Corresponding Author: Dept of Computer Science and Engineering, Sastra University, TamilNadu, India. (thanujaramai@gmail.com)
* Dept of Computer Science and Engineering, Sastra University, TamilNadu, India.
Received: December 5, 2017; Accepted: May 6, 2018

system for intrusion detection and prevention in a Tactical MANET environment. The proposed mechanism acts as a key line of defense against major security attacks in MANET. It exhibits computational intelligence [10-13] through fast unsupervised learning using fuzzy inference rule-based engine to protect MANET against variety of attacks and counter attacks. Our proposed methodology was evaluated using prototype – a proof of concept developed using MATLAB Simulink. The flexibility of using IBH_IDPS in Tactical mobile Ad-hoc network was evaluated using the prototype. Experimental analysis shows the proposed approach to be an attack resistant IDPS with assured high delivery ratio, low end-to-end delay [14], less computational complexity compared to existing schemes. Performance analysis proves the proposed approach to be more reliable and secure on devices and with good potential to be implemented in Tactical MANET.

The rest of the work is organized as follows: in Section II, related previous work is discussed; in Section III detailed illustration of the proposed system is provided. Section IV presents an evaluation of the system in terms of its performance. In Section V, the paper concludes along with a discussion on future directions.

2. Related Works

Many researches [15-21] have been done related to this topic, while the change in architecture and topology [23, 24] makes it essential to design and develop IDS specific to Tactical MANETs.

Research on intrusion detection techniques such as Watchdog [24] was used to detect malicious node behavior by listening to its next hop's transmission. The Watchdog node overhears and increments the failure counter if its next hop node fails to transmit the packet within a specific time slot. In this approach, when the count exceeds threshold value, the next hop node is considered to be a misbehaving node. Though this scheme proves to be efficient, it fails to detect misbehavior when the transmission power is limited. Variations in transmission power among nodes lead to inaccurate monitoring and false accusation in Watchdog. To overcome drawback of Watchdog, Liu et al, proposed TWOACK [25] to detect misbehaving nodes. In this approach, when a packet is received by each intermediate node an acknowledgement is sent back to the source. Acknowledgement is sent for data packet transmitted over every three consecutive node along the path from source to destination. Drawback of this scheme is unwanted network overhead caused due to transmission of acknowledgement packets. Such redundant transmission process can easily degrade the life span of the entire network. Additionally, there was no mechanism proposed in this scheme to verify the authenticity of the forged acknowledgement packets.

To overcome vulnerability caused due to forged acknowledgement packets, it becomes extremely important to ensure that all acknowledgement packets in acknowledgement-based schemes are untainted and authentic. Enhanced Adaptive ACKnowledgment based Digital Signature with message Recovery Algorithm - EAACK (RSA) [26] incorporates digital signature to all acknowledgement packets before they are transmitted. These packets are verified when they are accepted to ensure integrity of the Intrusion Detection System (IDS). It also verifies if the reported missing packet is received by the destination in a different route through authentication. Drawback is digital signature authentication adds to extra resource utilization. Primarily, most of the existing approaches assume that all the nodes in the network are cooperative, and thus do not address security issues caused due to these assumptions. Adaptive detection three ACKnowledgments (A3ACKs approach [27] aims in solving significant problem such as collaborative attacks. Especially when two consecutive collaborative misbehaving nodes reside in a route path, existing schemes assume that these misbehaving nodes cooperatively forward the routing packet instead they drop it. In A3ACKs model, every four consecutive nodes in path work together where the fourth node (three hops away from the first one) has to send back an acknowledgement packet to the first node in that group within a predefined time. Though this behavior makes the scheme handle issues caused due to collaborative misbehaving nodes, the overheads caused due to acknowledgement packets tend to reduce the overall network performance.

Dynamic nature of the environment, limited bandwidth, overhead associated with IDS not only makes most existing approaches inadequate to detect and prevent intrusions but also makes it difficult in sustaining network performance [28-31] and Quality of Service(QoS) of the system. While the distributed and centralized module implementation in proposed system helps to detect vulnerabilities and acts as a key line of defense in preventing major security attacks and sustaining the performance.

3. System Description

Let us consider the proposed IBH_IDP System where mobile nodes (like tanker, man pack radio and a military jeep) with varied transmission power, communication capability etc., are randomly distributed and connected with each other. The system is virtually grouped to self-organize and re-configure by itself to any variations without manual interventions. Initially the nodes in network are split into virtual groups. Each group comprises of optimal number of nodes (N_o). Node with high score from each virtual group is selected as a Virtual Head Node (VHN) or Intelligent Client Agent (ICA). The ICA's are distributed across the network whose role is to monitor, identify and report members who violate security rules to the server - the Command Control Center (CCC). The CCC is also referred as Smart Server (SS) is the most vital part of the

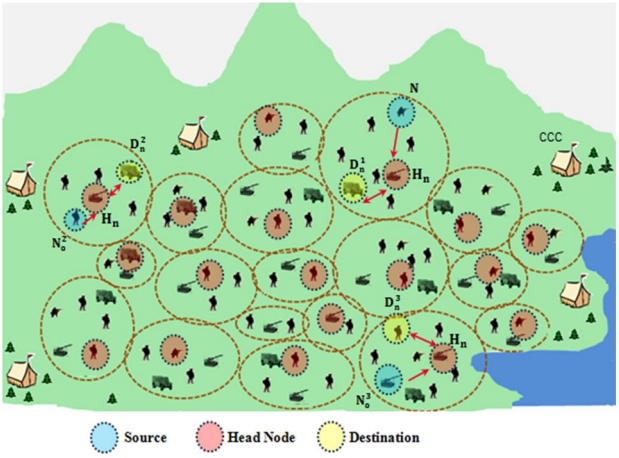

Fig. 1. Network Model of IBH_IDP System

Table 1. Summary of notations used in IBH_IDP system

Notation	Description
N_n^i	i^{th} Normal Node
H_n^i	i^{th} Head Node
T_n^i	Transmission power of i^{th} normal node
SC_n^i	Storage capacity of i^{th} normal node
M_n^i	Memory of i^{th} normal node
H_{count}	Head node total count value.
S_n^i	i^{th} Source Node
D_n^i	i^{th} Destination Node
M_n /M_{node}	Monitoring node
m_n/m_{node}	Monitored node
#(∗, m_n)	Number of incoming packets on m_n.
#(m_n,n_h)	Number of outgoing packets from m_n of which n_h is the next hop.
#(m_n, *)	Number of outgoing packets from m_n.
#([m_n], *)	Number of outgoing packets of which m_n is the source.
#(m_n, n_h)	Number of outgoing packets from m_n of which n_h is the next hop.
#([S_n],M_n,m_n)	Number of packets that are originated from S_n and transmitted from M_n to m_n.
#([S_n],D_n])	Number of packets received on m_n which is originated from S_n and destined to D_n.

system which is empowered with intelligence of fuzzy inference (FI) engine. The FI engine performs computation to determine at a granular level, the key line of defense to withstand and prevent unethical attacks and impart counter attacks. Role of smart server is to detect unusual network instances across network and initiate a global response to prevent such intrusion. Overall an ICA is used as a decision processing unit and SS is used as a decision making unit. The Network model of the IBH_IDPS is shown in Fig. 1.

The proposed IBH_IDP System architecture includes the following main components:

Normal Node(N_n): Nodes that communicates with other nodes to exchange information. These nodes form the members of the virtual groups. The local data and head node's identity is maintained in normal node's Local Aware Table (LAT).

Head Node (N_{head}) or Intelligent Client Agent (ICA): Node with high score is elected as head node of a virtual group. It is also referred as Intelligent Client Agent (ICA). It monitors activities and notifies CCC when an unusual activity is determined for further investigation.

Command Control Centre (CCC) or Smart Server (SS): It is the most vital part of the IBH_IDP System. It is empowered with fuzzy inference service engine capability that exhibits computational intelligence to dynamically classify unusual incidents either as normal or abnormal. Fuzzy inference service enhances classification accuracy and proves highly efficient in securing Command Control Communication and Intelligence (C3I) system. Notations used in IBH_IDPS are summarized in Table 1.

The IBH_IDP System consists of the following phases:

Phase I - Intelligent Client Agent Selection and Registration Mechanism

Phase II - Unethical Attack Detection and Prevention using Smart Server's Fuzzy Inference Mechanism

3.1 Phase I - Intelligent client agent selection and registration mechanism

During this phase, the IBH_IDP System performs two important activity. Initially it forms virtual groups to select the ICA node and then initiates ICA node registration mechanism.

Virtual Group Formation and ICA selection Process:

During this stage, nodes are selected randomly to initiate the virtual group formation process to divide the whole network into virtual groups. Virtul group formation is based on the following criteria: i) Number of nodes in each group should limit to an optimal range (N_o) depending on the coverage area. ii) Nodes in each group should be within the transmission range. iii) Overlapping between groups should be avoided to prevent anonymous node formation. Using information stored in LAT, score for each node is calculated and compared with each other to elect a virtual head node (node with high score is elected as the head). The VCH or ICA is allocated with additional functionality to monitor and notify on unusual activities to the CCC. Steps referred below illustrates the mechanism involved in virtual group formation and ICA selection mechanism:

Step 1: Prior to data packet communication, neighbor node discovery process is initiated. During this stage, each node ($\mathbf{N_n^i}$) broadcasts a "HELLO" message consisting of System Information Message (SIM) such as node's - identity ($\mathbf{N_{id}^i}$), mobility ($\mathbf{N_{mo}^i}$), computing capability ($\mathbf{N_{cp}^i}$), memory capacity ($\mathbf{N_{mc}^i}$) etc.

Step 2: Neighbor nodes that resides near to the broad-casting node receives the "HELLO" message. It records the sender's node SIM data in its Local Aware Table (LAT) and sends back an "ACK_HELLO" message. Nodes that reside within transmission range records the SIM information of its neighbors.

Step 3: Using SIM information recoded in LAT, each node calculates the score. Node with low mobility, greater computation capability and high memory capacity is given the maximum score. By comparing the score among each other, node with highest score is selected as the ICA node.

Step 4: Node selected as ICA node propagates "Group_ Formation" message to its neighbors. Neighbors receives the "Group_Formation" message, respond back by sending "Confirmation" message and become part of the virtual group. Any further virtual group formation messages received by neighbors are discarded and ICA node registration process is triggered.

Intelligent Client Agent node Registration Process:

Followed by the ICA node selection activity, IBH_IDP system performs the following steps to register the ICA node at the CCC or SS.

Step 1: The Intelligent Client Agent sends ICA registration (ICA_{reg}) message to centralized SS. Upon receiving the ICA_{reg} message, SS registers the ICA node in the ICA registration list (ICA_{reg_list}) maintained by the server. The list consists of the ICAs selected (along with its registered members) across the network.

Step 2: SS is empowered with fuzzy inference engine to significantly classify incidents received from ICAs, either as white, black or grey list candidates using predefined rule base specification.

White List (W_{list}) candidates: It indicates the list of nodes with valid IP and valid Port that are permitted to communicate with registered nodes in the group.

Black List (B_{list}) candidates: It indicates the list of nodes with invalid IP and invalid Port that are prevented from communicating with other nodes that reside in the virtual group.

Grey List (G_{list}) candidates: It indicates unknown IP and unknown Port that are prevented from communicating with nodes in the virtual group until authenticated as valid IP or Port by CCC.

Step 3: SS generates rule set (SS_{rule}) to incorporate new rules that does not exist currently in its rule base specification (REG_{rule_base}). Using the updated rule base, registered candidate list (REG_{cand_list}) is generated. The REG_{rule_cand} message with updated candidate list (REG_{cand_list}) is sent to all ICAs across the network.

Step 4: ICAs upon receiving the REG_{rule_cand} message initiates candidate registration process to update its Local Aware Table (LAT) and Global Aware Table (GAT). Each ICA also maintains a GAT which contains the following: i) latest list of white and black candidates (set as per the REG_{rule_cand}). ii) List of head node's identity information across network (used for route detection)

Step 5: Apart from performing the candidate registration mechanism, the ICA also enables a light weight autonomous IDS client module within itself. This client IDS process ensures validating authentic members within group to communicate with each other.

Step 6: Members in each group verify their authenticity with its ICA. Only valid authenticated members are allowed to perform data communication otherwise the request for data communication is rejected by the ICA.

Validity of member verification is performed by ICA as follows :

Case 1 : If a registered member node "A" within group "G1" needs to communicate with another registered member node "B" that belongs to same group "G1" provided, the head node of the group is "H1" then,

- Node "A" sends a message to its head node "H1"
- From the message, "H1" reads the source and destination nodes identity and looks-up its LAT to verify if the source and destination node id exists (as per the registered candidate list).

  If both source node "A" id and destination node "B" id exist in H1 node's LAT then

  "H1" sends "success" notification message to node "A", allowing data communication between node "A" and node "B"

  end;

Case 2 : If a registered member node "A" within group "G1" needs to communicate with another registered member node "B" that belongs to another group "G2" provided head node of group "G1" be "H1" and the head node of Group "G2" be "H2" then,

- Node "A" sends a message to its head node "H1"
- From the message, "H1" reads the source and destination nodes identity and looks-up its LAT to verify if the source and destination node id exists. As per the case considered, source node id "A" would exist in the LAT of H1, while destination node id "B" would not. Hence, "H1" will now look-up its GAT which contains the global list of head node ids along with its registered member list information.
- If destination node "B" id exist in H1 node's GAT then

  "H1" sends "success" notification message to node "A", allowing data communication between node "A" and node "B";

  end;

Case 3 : For any new members with unknown IP or Port apart from the registered list the incident is set to be abnormal and notified by ICA's to CCC for further authentication. If an unregistered node "U" initiates communicate request to a registered member node "B" that belongs to group "G1"provided head node of group "G1" be "H1" then,

- Node "U" (source) sends a message to node "B"
- Node "B" (destination) upon receiving the message from node "U", it forwards the request to its head node "H1" for authorization.
- "H1" looks-up its LAT to verify if source and destination nodes identity exists. As per the case considered, destination node id "B" would exist in the LAT of H1, while source node id "U" would not. Hence, "H1" will now look-up its GAT which contains the global list of

head node ids along with its registered member list information.
If node id "U" id does not exist in H1 node's LAT and GAT then
"H1" sends "failure" notification message to node "B", rejecting data communication between node "B" and node "U";
"H1" notifies the information regarding the invalid node's identity to CCC for further verification.
end;

The CCC receives the message and verifies its existing registered candidate list. If the node "U" does not exist in list maintained by the server, it adds the node Id, IP and Port to its black listed candidate list. CCC sends notification regarding the new black list candidate to all ICA across the network. All ICAs receives the message and updates its LAT and GAT.

Algorithm 1 summarizes the steps involved in Intelligent Client Agent Selection and rule registration mechanism

Algorithm 1: ICA Selection and Rule Registration Mechanism

Initialize $\mathbf{N_n^I}$, $\mathbf{N_{id}^i}$, $\mathbf{N_{mo}^i}$, $\mathbf{N_{cp}^i}$, $\mathbf{N_{mc}^i}$;
/*Node_I=$\mathbf{N_n^I}$,Node_J=$\mathbf{N_n^J}$,Node_ID=$\mathbf{N_{id}^i}$,Mobility=$\mathbf{N_{mo}^i}$,Computing_Capability=$\mathbf{N_{cp}^i}$, memory capacity =$\mathbf{N_{mc}^i}$ */
$N_n^I \rightarrow H_{msg}$; // Node_I broadcasts Hello msg
If ($H_{msg} \leftarrow N_n^J$) then //If Node_J receives Hello msg of Node_I
//fetch the identity of Node_I and store in LAT of Node_J
LAT_J = get_identity(N_n^I);
$N_n^J \rightarrow AckH_{msg}$; // Node_J sends Ack msg
// If Node_I receives Ack msg from Node_J
If $AckH_{msg} \leftarrow N_n^I$) then
//fetch the identity of Node_J and store in LAT of Node_I
LAT_J = get_identity(N_n^J);
end;
end;
// scores of nodes are calculated to find the highest score
H_{score} = get_higest_score (calculate_score(LAT_I));
// node with highest score is identified
N_n^i = getNode(H_{score});
// verify if the node with highest score satisfies the ICA norms and best among them is selected as the ICA node
If($N_n^i N_{mo}^i \leq M_\delta$)&&($N_n^i Tp_{VCH}^n \geq Tp_\delta$)||($N_n^i \mathbf{N_{cp}^i} \geq Cp_\delta$)&& ($N_n^i \mathbf{N_{mc}^i} \geq Mem_\delta$) then
StoreData =$Best_{VH}$;
N_n^{head} = Get_Head_node($Best_{VH}$);
end;
set_head_node (N_n^{head}); //ICA node is selected
$N_n^{head} \rightarrow GrpF_{msg}$ ($N_n^{neighbor}$); //Group formation msg is sent
$N_n^{neighbor} \leftarrow Cnf_{msg}$ (N_n^{head}); //Confirmation msg is sent
$N_n^{neighbor} \rightarrow GrpFrm_{msg}$;
$ICA_{reg} \rightarrow CCC$; //ICA registration is initiated to CCC
register(ICA_{reg}); initiateSS_{rule}( ); // SS generates rule set
updateRule(REG_{rule_base}); updateREG_{cand_list} ( );
$CCC \rightarrow REG_{rule\_cand}$;
$ICA \leftarrow REG_{rule\_cand}$; update LATGAT(REG_{rule_cand});
Enable_CIDS(TRUE); // ICA enables client IDS module
While ($N_A \leftarrow N_B$)
verify(EG_{rule_cand});
// ICA validates authenticity of members
// Caase 1
if ($N_{B\_ipp} == W_{list}$) then
H1 = approve(N_B req);
$N_A \rightarrow N_B$;
end;
// Case 2
if ($N_{B\_ipp} == B_{list}$) then
H1 = reject(N_B req);
end;
// Case 3
if ($N_{B\_ipp} == G_{list}$) then
H1 = fwdICA(N_{B_ipp});
if ($N_{B\_ipp} \neq$ GAT) then
H1 = reject($N_A N_B$req);
H1 $\rightarrow$ CCC;
end;
end;
end;

At CCC the server enabled IBH-IDPS service engine parses the instances using FIS process.

Nevertheless, when the available evidence is inconclusive, ICA aggregates such incidents and forwards to CCC for evaluation. As the registered rules REG_{rule_cand} can detect only known attacks, IBH_IDP System implements an effective fuzzy inference engine specification at the server that exhibits computational intelligence to dynamically classify unusual incidents to enhance classification accuracy and proves highly efficient in securing C3I system.

3.2 Phase II - Unethical attack detection and prevention using smart server's fuzzy inference mechanism

Most of the existing IDPS are designed to tackle a particular category of network attacks, as they are implemented on top of existing protocols. As number of new security risks increases in MANET, it becomes hard to distinguish known or unknown threats and defense those using existing schemes. Unknown attacks should be detected and prevented before they harm the network. IBH_IDPS primarily uses unsupervised learning mechanism as it significantly learns, analyzes and classifies unknown incidents either as white, black or grey list candidates using its clearly defined fuzzy inference specifications. Fast mining and categorization makes the proposed approach unique and well suited for Tactical battlefield environment.

In this phase, CCC or SS receives aggregated message from ICA and forwards it to FI engine for processing. Fuzzy inference engine classifies instances either as

normal or suspected, making it desirable for the security administrator for decision making. The IBH_IDPS at SS,

- converts raw data into standard format
- discovers relationship among instances and generates rules (set of if-then rules) for classification
- maintains a knowledge base – a working memory of derived facts
- constitutes of fuzzy inference engine containing the reasoning logic used to process the knowledge base.
- provides a decision support and reporting mechanism

Aggregated messages received as raw information are converted into standard format. Content of the packet header is parsed, encoded and stored (as incidents) into stationary database. Each features of the packet header content is investigated to ascertain the healthiness of the network. Primarily, for investigating suspicious activities in time critical networks, we have considered the IP address and Port number as verification parameters - all other relevant features such as time, length, sequence number etc., can be evaluated to enhance the system. Using the similarities (such as type of attack, time of attack, attack sources etc.,) and relationship that exist between incidents, new set of rules are created and added into knowledge base. The rules are generated based on pre-defined norms for known attacks and dynamically generated for unknown attacks. Rules act as a knowledge base for inference reasoning, semantic information handling, and event correlation. Apart from packet's header information, traffic related patterns and features, routing operations, statistics are used for creating rules and detecting intrusions. Based on existing rules set, derived statistics is considered to be an attack if it deviates from pre-computed results. If variance or deviation is identified, further investigation is done using fuzzy inference rule-based processing engine using set of identification rules to determine the type of attack and attacking node. Sample rules used to determine known attacks are:

Rule to determine black hole attack: This rule uses information available on the monitoring node (M_{node}). Global Forward Percentage (GFP) is used to detect black hole attack. Let $N(M_{node})$ denote Mnode's 1-hop neighbors.

$$GFP^{\,s\_node}_{\,m\_node} = \frac{\#^L(*,Mnode) - \#^L(*,[Mnode])}{\sum_{i \epsilon N(Mnode)} \#^L(i,Mnode) \; - \sum_{i,j \epsilon N(Mnode)} \#^L(i,[j]) - \#^L(*,Mnode)}$$

If (packets(N(M_{node})) → Other_nodes) || N(M_{node})≠0) &&($GFP^{\,s\_node}_{\,m\_node} = 1$*) then*
blackhole attack detected = true;
attacker Node = M_{node}*;*
end;

Rule to determine unconditional packet dropping: This rule uses Forward Percentage (FP) over a period L to define the attack.

$$FPm_{node} = \frac{\#^L(mnode,Mnode) - \#^L([mnode],Mnode)}{\#^L(Mnode,mnode) - \#^L(Mnode,[mnode])}$$

If (packets to be forwarded ≠ 0) && ($FPm_{node} = 0$*) then*
unconditional packet dropping attack = true;
attacker = m_{node}*;*
end;

Rule to determine selective packet dropping: This rule uses Local Forward Percentage (LFP) for each source S_{node}.

$$LFP^{\,s\_node}_{\,m\_node} = \frac{\text{packets from source s actually forwarded}}{\text{packets from source s to be forwarded}} = \frac{\#^L([snode],mnode,Mnode)}{\#^L([snode],Mnode,mnode) \; - \#^L([snode],Mnode,[mnode])}$$

If (packets from source to be forwarded ≠ 0) && ($LFP^{\,s\_node}_{\,m\_node} = 0$*) then*
unconditional packet dropping detected = true;
attack Targeted Node = s_{node}*;*
else if ($LFP^{\,s\_node}_{\,m\_node} < LFP_{Thres}$*)then*
random packet dropping detected = true;
attack Targeted Node = s_{node}*;*
else
no attack detected;
end;

For each features, solution is derived and stored into the archive rule set. Fuzzy Inference Engine (FIE) uses the archived rule set to search and verify features and generate a response (solution). For an incident, FIE verifies the rule set to generate a response. For known features (known problems or known attacks), as per the pre-defined rules response is generated. While for unknown features (unknown problems or unknown attacks - combination of multiple or new attacks), new rules are generated and added to the rule set archive for future verification (rather than generating new rules every time when such problems are detected). This property of unsupervised self-learning mechanism dynamically adds intelligence by enhancing

- the self-organizing behavior of the system
- the ability to adapt to the environment dynamics and
- the potential to detect and combat unknown attacks
- thereby making the proposed system inevitable for Tactical MANET environment. Detailed specification regarding Smart Server's fuzzy inference service engine functionality is elaborated in the following section.

Smart server's fuzzy inference service engine functionalities:

The IBH-IDP system comprises of a Smart Server (SS) empowered with an advanced intelligence of fuzzy inference service engine. Fuzzy inference mechanism is an error-tolerant, Artificial Intelligence technique that deals with unordered sets of different cardinalities and well suitable for time critical applications.

Mathematical Model for analysing Fuzzy Sysstems:

The fuzzy mathematical principles are developed by replacing the sets in classical mathematical theory with fuzzy sets (FSs). Fuzzy variables are processed using a system called a fuzzy inference system (FIS) which involves fuzzification, fuzzy inference, and defuzzification. The FIS collects the rules in the fuzzy rule-base into a mapping from fuzzy set A∈X to fuzzy set B∈Y. We must construct interfaces that are the fuzzifier and defuzzifier, between the FIS and the environment because in most applications the input and output of the FS are real valued numbers.

Let the sets A and B are a fuzzy sets, x_h (h=1,…,6) are an input variables, y is the output variable, and i, (i=1,…,I), is the number of rules. The fuzzy set A consists of, $A_1{}^{j1}$,…, $A_6{}^{j6}$, fuzzy subsets. It is called linguistic terms that represented by triangular Membership Functions with b=c. The fuzzy operator "and" (t-norm) is used to connecting between linguistic terms in each rule of the model. The function $f^{j1\cdots j6,}$ (x_1,…,$_6$) is a linear function depends on inputs x_k. The first five linguistic terms are represented by $A^{ji}{}_h$ (j_i=1,2,...,5) that depends on linguistic variable x_h (h=1,...,5), Consider the general membership function of fuzzy set, A, is a continuous function in R given by:

$$\mu\,(x; a, b, c, d) = \begin{cases} 0 & \text{if } x < a \\ a(x) & \text{if } a \le x < b \\ 1, & \text{if } b \le x \le c \\ d(x) & \text{if } c < x \le d \\ 0 & \text{if } d < x \end{cases}$$

where $[a,d] \subset R$ *and* $a \le b \le c \le d$, $0 \le a(x) \le 1$ a non-decreasing function is $\in [a,b)$ *and* $0 \le d(x) \le 1$ is a non-increasing function $\in (c,d]$.

If fuzzy sets $A^1,^2,\ldots,A^N \in W \subset R$ then, they are called:

1. Complete on W, if there exists A^k such that $\mu(x) > 0$, for any $x \in W$.

2. Consistent on W if $\mu_A{}^k\ x = 1$ for some $x \in W$ implies that $\mu_A{}^j\ x = 0$, for all $k \neq j$.

3. Normal, consistent and complete with general MFs, $\mu_A{}^j\ (x;,b_j,c_j,d_j)$. If $A^1 < A^2 < \cdots < A^N$, then $c_j \le a_{j+1} < d_j \le b_{j+1}$, for j=1,2,…,N−1.

In IBH_IDPS, fuzzy inference logic is designed by considering multiple attack types as the crisp input. Our scenario considers Global Forward Percentage (GFP), Forward Percentage (FP) and Local Forward Percentage (LFP) as its input. These inputs act as the vital sign to predict the type of event caused in the network. The next step is to fuzzify the input variables through fuzzification. The process of mapping a crisp value of an input to membership degrees in different Fuzzy Linguistic variables is referred to as fuzzification. Fuzzy sets have to be determined to fuzzify the variables, ie., for each input variable the corresponding range of fuzzy set have to be determined. Threshold value for range is set as per the application scenario. In our case it has been set as low, medium and high (T_{low} T_{med} T_{high}) limit. The formation of fuzzy set is through classification of data with its corresponding membership functions. Table 2 describes the classification of input variables for "Black Hole", "Unconditional Packet Dropping" and "Selective Packet Dropping" attack and its fuzzy set.

Table 2. Classification of Attacks

GFP	FP	LFP	Risk Level(RL)
L	L	L	RL_{low}
L	H	L	$RL_{moderate}$
M	M	H	RL_{high}
M	H	L	$RL_{moderate}$
M	L	L	RL_{low}
H	L	H	RL_{high}
M	M	M	$RL_{moderate}$
H	H	H	RL_{high}

Table 3. FIS crisp output derived using GFP, FP and LFP

Input field	Range	Fuzzy set
Local Forward Percentage (LFP)	T_{low}	Low
	T_{med}	Medium
	T_{high}	High
Forward Percentage (FP)	T_{low}	Low
	T_{med}	Medium
	T_{high}	High
Global Forward Percentage (GFP)	T_{low}	Low
	T_{med}	Medium
	T_{high}	High

Fuzzification is followed by fuzzy rule base creation process. Fuzzy rule base is created using logical combination of input variables with AND operator. Quality of results in a fuzzy system depends on the fuzzy rules. For example, rule base using GFP, FP and LFP variables are as follows:

If (GFP==‘low’)&&(FP==‘low’)&&(LFP==‘low’)then
RL = RL_{low};
if (GFP==‘low’)&&(FP==‘high)&&(LFP==‘low’) then
RL = $RL_{moderate}$;
If (GFP==‘med’)&&(FP==‘med)&&(LFP==‘high’) then
RL = RL_{high}
If (GFP ==‘med’)&&(FP==‘high’)&&(LFP==‘low’) then
RL = $RL_{moderate}$;
If GFP ==‘med’)&&(FP==‘low’)&&(LFP==‘low’) then
RL = RL_{low};
If (GFP==‘high’)&&(FP==‘low’)&&(LFP==‘high’) then
RL = RL_{high};

In IBH_IDPS, we have considered 3 fuzzy sets - RL_{low}, $RL_{moderate}$, RL_{high} to determine the Risk Level(RL). Inference engine uses the rule base and by inferring rules generates the fuzzified values. Table 3 displays the fuzzy rules corresponding to the parameters used for decision making process.

Risk Level determined using fuzzy rule set are the output variables. Effective decision making using rule

base results in crisp output: RL_{low} or $RL_{moderate}$ or RL_{high}. The idea behind fuzzy inference engine is to reduce the complexity and make rule mining efficient for classification based on the following criteria's:

Criteria 1: If crisp output for incidents is RL_{low}, then those are classified as "White list" candidates. The deviations or variances derived for these incidents are below the allowable range, such incidents are classified as "White or Good" candidates.

Crit*eria 2:* If crisp output for incidents is RL_{high}, then those are classified as "Black list" candidates. The deviations or variances *derived* for these incidents are above the allowable range, such incidents are classified as "Black or Bad" candidates.

Criteria 3: If crisp output for incidents is $RL_{moderate}$, then those are classified as "Grey list" candidates. The deviations or variances derived for these incidents are said to be within the allowable range, such incidents are classified as "Grey" candidates.

Due to unavailability of adequate information (rules), incidents may not be classified either as "good" or "bad", such incidents are set as "grey" candidates. These incidents are categorized either as "good" or "bad" labeled candidates when adequate information satisfying the said criteria is met in future. High computation and rule mining capability of the fuzzy inference engine classifies incidents appropriately as it employs intelligence at granular level to determine the crisp output in selecting the best suitable candidates. An accurate estimate of crisp output (the risk level) helps in securing the system by achieving better reliability and lower latency. Algorithm 2 details the steps involved in Fuzzy inference rule-based processing and crisp output classification

Algorithm 2: Rule-based processing using fuzzy inference engine and crisp output classification

Input: GFP, FP, LFP are provided to FIS engine. IBH_IDPS performs FIS process to generate the most suitable crisp out for candidate classification.

Initialize $incidents_{count} = 0$;
for each $incident_{data}$
    if (($incident_{data}$== $S_{relationship}$) then
        $Ic_{suitable\_list} = Ic_{suitable}$;
        $incidents_{count} = incidents_{count} + 1$;
    else
        $incidents_{ignore}$ = true;
    end
end;
for each $incidents_{count}$
$Ic^{i}_{process} = Ic_{suitable\_list}(i)$;
    if (($Ic^{i}_{process}$GFP== L) && ($Ic^{i}_{process}$FP==L)&&
($Ic^{i}_{process}$LFP== L) then
        $CP_{output} = RL_{low}$;
    else if (($Ic^{i}_{process}$GFP== L) && ($Ic^{i}_{process}$FP==H) &&
($Ic^{i}_{process}$LFP== L) then
        $CP_{output} = RL_{moderate}$;
    else if (($Ic^{i}_{process}$GFP== M) && ($Ic^{i}_{process}$FP== M) &&
($Ic^{i}_{process}$LFP== H) then
        $CP_{output} = RL_{high}$;
    end;
end;
if (CP_{output} == RL_{low}) then
    $Ic^{i}_{classify} = C_{good}$;
else if (CP_{output} == RL_{high}) then
    $Ic^{i}_{classify} = C_{bad}$;
else
    $Ic^{i}_{classify} = C_{grey}$;
end

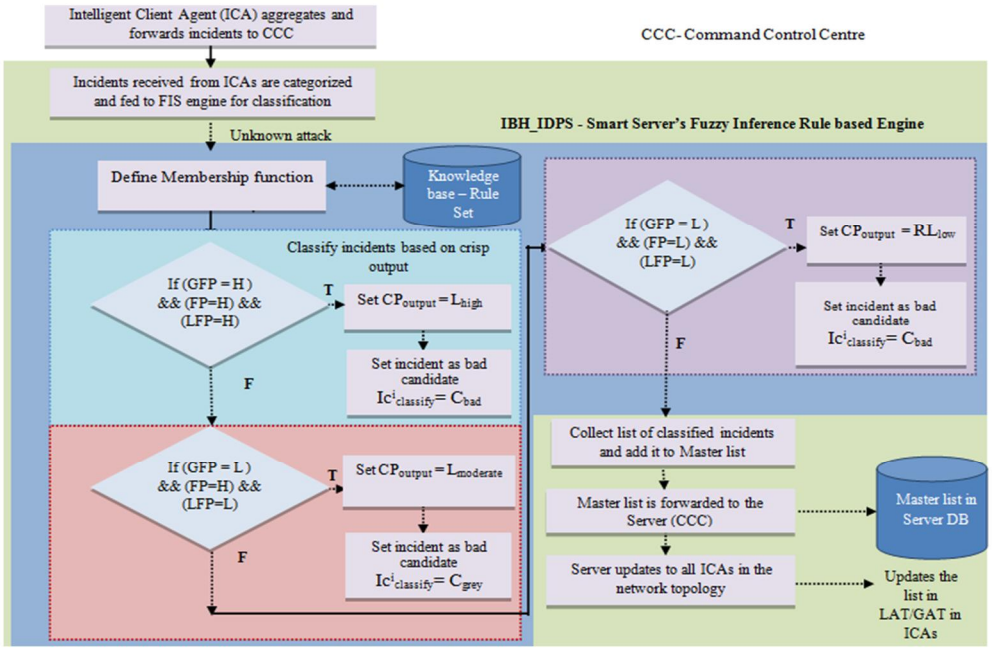

Fig. 2. Flow model of IBH_IDP System

Output: Most suitable classification – either as good or bad or grey listed candidate is selected and set to incidents.

The flow model of IBH_IDPS is depicted in Fig. 2. The results from the fuzzy rule-based engine are collected and sent from the CCC to all the ICAs across the network. ICA's on receiving the response updates it's LAT and GAT and forwards to all its registered members for updating its LAT. Using the updated list, ICAs authenticates data communication with the valid nodes (if it is found to be valid or white listed candidate) and rejects communication with invalid nodes (if it is found to be a invalid or black listed candidate). Almost all activities detected locally are thus logged to the centralized system and distributed across the network. The inspection of these logs not only allows intrusions to be detected and prevented, but also helps to analyze and audit (determining the extent of damage occurred, trace back attack, recording the attack patterns) incidents or events for real-time detection and prevention exploiting the functionality of the proposed system more suitable for Tactical MANET.

4. Simulation Results

Performance of the proposed IBH_IDP System is evaluated by developing a prototype using MATLAB Simulink. Our experimental analysis considers set of MANET nodes deployed in simulation area of 1000m X 1000m as shown in Fig. 3.

With radius set to vary until 100 meters, virtual groups are formed. Nodes (~5% - ~10%) in each group, communicate among each other to elect a virtual head node. Every registered members of the group is directly communicable to its virtual head node. At varied time slot during simulation, nodes are randomly chosen to act as source (node that generates message and transmits the message to destination). Nodes mobility is varied between 0m/s to 25m/s. Reference Point Group Mobility Model (RPGM) with physical layer speed of 1Mbps to 2Mbps is considered. The desired delivery rate set to be 99% (very high) and 85% (medium). To better investigate the scope and performance of the proposed IBH_IDPS approach in handling security vulnerabilities, we have chosen Watchdog [24], TWOACK [25], EAACK (RSA)[26] and A3ACKs [27] as existing representative protocol for comparative analysis. Performance was evaluated using the following scenario:

Scenario - A malicious node with black hole attack was introduced into the network which absorbs legitimate data packets and drops the same causing huge loss of information across network.

Packet Delivery Ratio (PDR): PDR defines ratio of the number of packets delivered to the destination successfully against the total number of packets generated by the source.

Scenario's PDR Analysis: The legitimate packets that pass through the malicious nodes are absorbed and dropped. PDR results for various approaches are referred in Table 4 and displayed in Fig. 4.

From Fig. 4, we can observe that with 10% of malicious node, IBH_IDPS surpassed Watchdog performance by ~20% - ~25%, and for TWOACK and EAACK (RSA) by ~2% - ~4%. Even when the number of malicious node increases IBH_IDPS is able to sustain malicious activity and deliver packets successfully to destination compared to other existing approaches. From the result, we can observe that TWOACK, EAACK(RSA) and A3ACKs scheme proves to be better than Watchdog in delivering

Table 4. Scenario – Packet delivery Ratio

Scenario's : Packet Delivery Ratio					
	MN: 0%	MN:10%	MN:20%	MN:30%	MN:40%
Watchdog	1	0.83	0.77	0.7	0.67
TWOACK	1	0.97	0.96	0.92	0.92
EAACK(RSA)	1	0.96	0.97	0.92	0.92
A3ACKs	1	0.97	0.96	0.94	0.93
IBH_IDPS	1	0.99	0.98	0.96	0.95

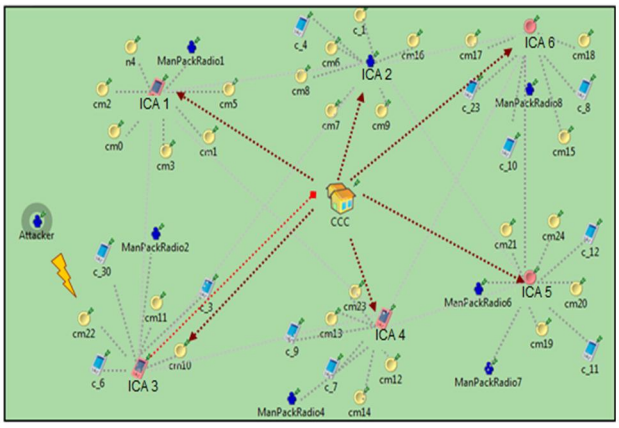

Fig. 3. Network model of IBH_IDP System

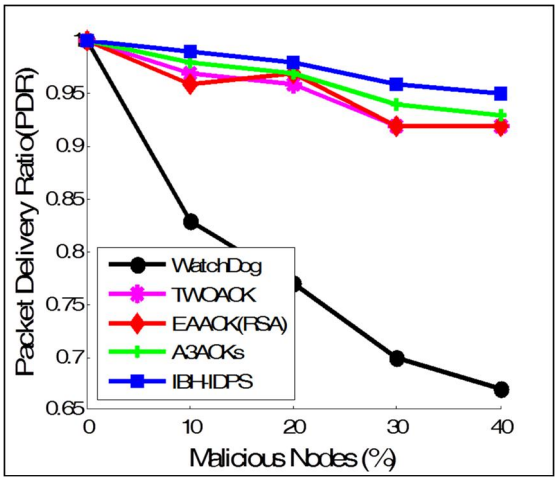

Fig. 4. Scenario's – PDR

packets successfully to destination using authenticated acknowledgement (identifies and eliminates corrupt nodes) whereas, these acknowledgement packets causes additional delay in these approaches degrading the performance of the network. ICA election in IBH_IDPS ensures authenticity during communication preventing malicious activities. These ICAs permits data communication only among registered members and avoids unregistered members to become part of the virtual group unless authenticated by CCC. This not only ensures successful data delivery among members but also prevents delay caused during communication. Legitimate communication in proposed approach is enhanced to sustain high PDR even with low transmission power and in collision constrained setup.

From the results, we can see that IBH_IDPS can guarantee the desired delivery rate even after the malicious node density reaches above a certain level.

Routing Overhead (RO): RO defines the number of routing related transmissions.

Scenario's RO Analysis: From the results shown in Table 5 and Fig. 5, the curves for various protocols (including IBH_IDPS) are plotted as the malicious node increases.

Fig. 5 shows that the routing overhead of A3ACKs, EAACK (RSA) and TWOACK rises as malicious node is increased. Primarily, increase in malicious node prevents legitimate packets to be transmitted to destination successfully as they are captured and dropped by these nodes. To overcome packet loss caused due to malicious activity, TWOACK, EAACK (RSA), A3ACKs scheme generates acknowledgment packets for verifying the authenticity of nodes at all levels for misbehavior detection causing high RO.

In contrast, the proposed IBH_IDPS displays overhead immunity similar to Watchdog. IBH_IDPS is empowered with additional functionality in ICA to monitor and handle false misbehavior activity within its group and notify those incidents to CCC for further investigation. As most ROs are handled by ICAs within each virtual group, the number of ROs being transmitted across entire network is reduced and makes this approach more preferable for Tactical MANET.

Table 5. Scenario - Routing Overhead

Scenario's : Routing Overhead					
	MN:0%	MN: 10%	MN: 20%	MN: 30%	MN: 40%
Watchdog	0.02	0.025	0.025	0.023	0.023
TWOACK	0.18	0.4	0.43	0.42	0.51
EAACK(RSA)	0.16	0.3	0.37	0.47	0.61
A3ACKs	0.14	0.17	0.19	0.25	0.49
IBH_IDPS	0.036	0.039	0.042	0.042	0.043

Computational Time and CPU Utilization: Computational Time defines the time taken by IBH_ IDPS process to analyze and classify incidents using fuzzy inference engine either as white or black or grey listed candidates. Fast unsupervised learning instantly classifies incidents and helps to reduce time taken during computation. Deep analytics using fuzzy inference rule-based process infers parameters to predict variance (minimum and maximum level) and optimal allowable range for dynamic categorization and helps IBH_IDPS to achieve low computational time compared to other schemes as shown in Fig.6. Average computational time of IBH_IDPS is ~15 % to ~20% faster than Watchdog and ~5% to ~8% faster than EAACK(RSA) and A3ACKs making it a better scheme.

With varied network traffic and mobility, the CPU consumed by IBH_IDPS on an average was 0.9%, whereas 70% to 80% of the CPU was consumed by Watchdog. As Watchdog IDS runs on all nodes under all conditions it results in high CPU consumption. Whereas, the proposed mechanism offers a significant improvement by efficiently utilizing limited resources by loading light weight IDS module only to intelligent client agents and leaving all

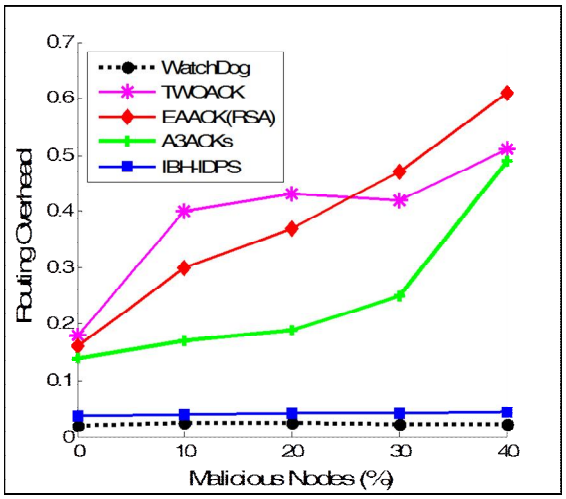

Fig. 5. Scenario's – Routing Overhead

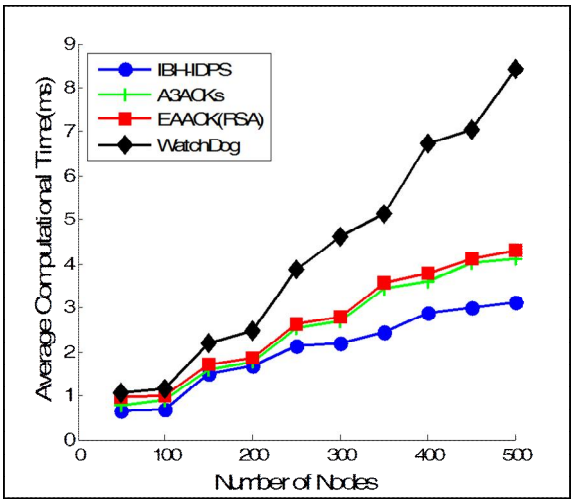

Fig. 6. Computational time Vs Nodes

other nodes to perform only its local activity.

End-to-End Delay: The Elapsed time between the time slot the packet is generated at its source and the time slot it is delivered to its destination. Delay metric plays a vital role in time critical application.

Packet generation from source, distribution via nodes and delivering to destination was analyzed through simulation process with varying node density (n), packet-broadcast probability q = {0.1, 0.2} and system load ρ = 0.6 (ρ = λ/μ, where λ maximum packet arrival rate and μ indicates per node throughput capacity). Results observed during the simulation is plotted in Fig. 7 indicates that the simulated end-to-end delay data goes along with the theoretical QBD- Quasi-Birth-and-Death [14] results. The observation indicates that the proposed IBH_IDP system's efficiency in sustaining low delay making it more suitable for tactical MANET. Also, from the observation it's found that as node density increases, contention of wireless channel access increases causing high end-to-end packet delay.

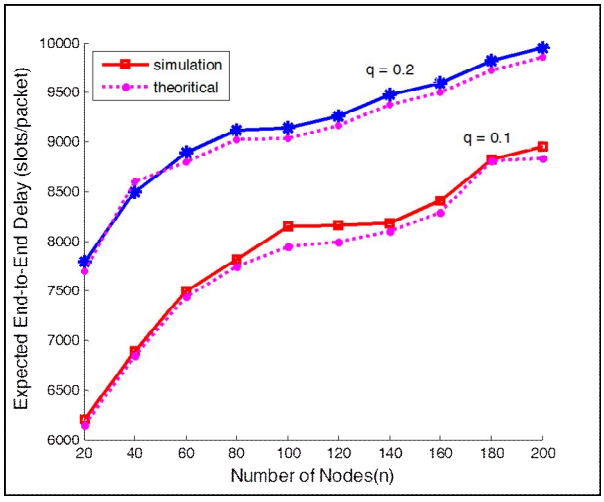

Fig.7. Packet End-to-End delay Vs Number of nodes

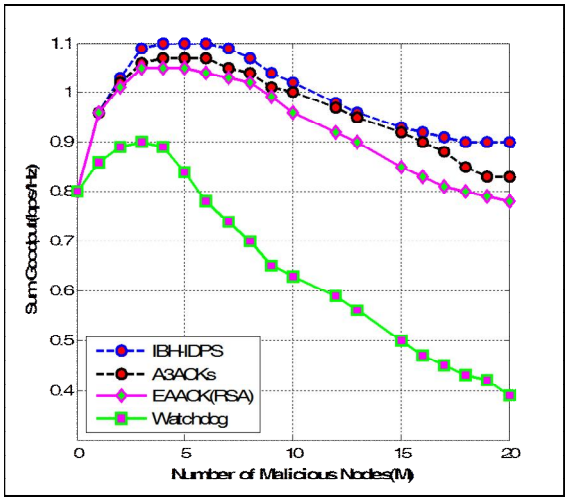

Fig. 8. Sum Goodput Vs Number of Malicious Nodes

Channel Utilization: Goodput refers to the total amount of data successfully delivered to the destination per unit time. The channel utilization of active nodes performing data communication was analyzed to identify the sum goodput of the network. During simulation, we assumed the traffic arrival probability be at a rate of ρ=0.5 (bps/Hz) by the source nodes. Goodput was analyzed by increasing the number of malicious nodes in the network. Simulation results were captured and plotted as shown in Fig. 8.

From the results it is observed that with increasing number of malicious nodes(increase in suspicious activity in network), Watchdog nodes fail to deliver packets successfully to destination causing degradation in sum goodput. The goodput (amount of data successfully delivered to the destination) is high when malicious nodes are low ($M < 5$). Optimal amount of goodput is achieved for all approaches when the malicious nodes are less between 0 to 5. Each source node accounts to loss of data packets (caused due to malicious nodes dropping the packets) as the malicious node level is increased decreasing the goodput. Even when the sum goodput is low when M>15, the difference between A3ACKs, EAACK(RSA) and IBH_IDPS is not very large compared to Watchdog. Successful data delivery is higher when M is between 6 to 8. Even in the presence of malicious nodes, using fuzzy inference rule-based processing, IBH_IDPS approach is able to combat new attacks and utilize the opportunities by trasmitting more violently to achieve better goodput. Higher goodput indicates nodes are able to combat unethical activities providing opportunities for more nodes to transmit data successfully to destination. The effectiveness of IBH_IDPS approach accommodates more nodes to achieve higher goodput both in normal and malicious node constrained environment. The combination of ICA's distributed functionality and Smart Server's fuzzy Inference rule-based effective decision making approach increases successful data transmission in MANET

Receiver Operating Characteristic Curve (ROC): The True Positive Rate (TPR) and False Positive Rate (FPR) are considered for deriving ROC. True Positive indicates an incident from registered (valid) node is captured and appropriately classified as white or black or grey candidate by IBH_IDP System's fuzzy inference rule-based approach resulting in a success. False positive indicates an incident from unregistered (malicious) node is captured and wrongly classified as white or black or grey listed candidate by IBH_IDP System's fuzzy inference rule-based approach resulting in a success provided the incident should actually have been rejected. TPR and FPR of IBH_IDPS , A3ACKs and EAACK(RSA) is shown in Fig. 9.

From the ROC curve referred in Fig. 9, we can observe that the attempt made by the registered node's success rate

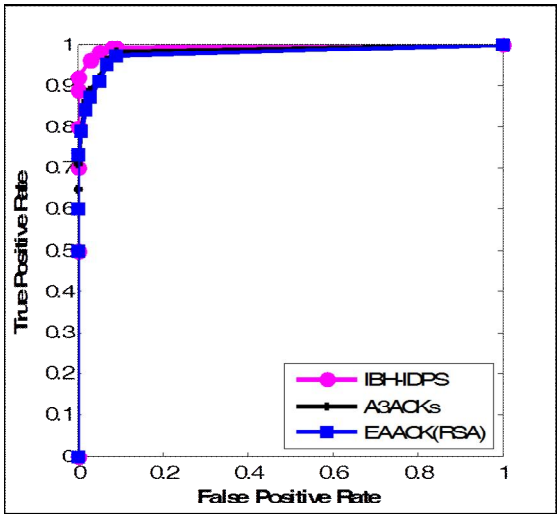

Fig. 9. ROC comparison between IBH_IDPS Vs A3ACKs and EAACK(RSA)

(TPR) is higher while the attempt made by the suspicious node's success rate is negligible. IBH_IDPS's ROC is better compared to A3ACKs and EAACK(RSA) as the distributed ICA's intrusion detection unit and Smart server's fuzzy inference rule-based decision making and intrusion prevention unit helps to analyze and classify unknown incidents appropriately ensuring higher security and integrity at the receiver.

5. Conclusion

Despite the rapid progress and the large volume of research activities made in the MANET, almost all research areas still impose many open issues. In this paper, we have proposed a novel "Intelligent Behavioral Hybridized Intrusion Detection and Prevention System" predominantly suitable for military operation in Tactical communication network. Primarily, the proposed scheme makes use of a virtual grouping technique and fuzzy inference rule-based service processing to protect Tactical MANET against variety of attacks and counter attacks. Simulation results proves that our architectural re-modification proves to be more effective, secure and robust when compared with existing methods as most existing methodologies do not assume extreme network architecture conditions. For successful implementation of an advanced Artificial Intelligence based IDPS system, our future work relies on challenges imposed in limitation on node density when number of node increases both in full and semi-MANET conditions.

References

[1] Su Ming-Ying et al, "Prevention of Selective Balckhole Attacks on MANETs through intrusion detection systems," *Computer Communications* (*ELSEVIER*), The Netherlands, pp. 107-117, 2011.

[2] Snehal, P. Dongarea; Mangrulkarb, R. S, "Optimal Cluster Head Selection Based Energy Efficient Technique for Defending against Gray Hole and Black Hole Attacks in Wireless Sensor Networks," *Procedia Computer Science,* 78 (2016), pp. 423-430, 2015.

[3] Xiang Wang, Xiaodong Song, "New Clustering Routing Method Based on PECE for WSN. EURASIP Journal on Wireless Communications and Networking," (162), pp. 1-13, DOI: 10.1186/s13638-015-0399-x, 2015.

[4] Si Liu, Ting Zhang, "Novel Unequal Clustering Routing Protocol Considering Energy Balancing Based on Network Partition & Distance for Mobile Education," *Journal of Network and Computer Applications*, vol. 88, no. 15, pp. 1-9. m2017, DOI:10.1016/j.jnca.2017.03.025

[5] Niu H L, Liu S, "Novel PEECR-based Clustering Routing Approach," *Soft Computing*, vol. 21, no. 24, pp. 7313-7323, DOI: 10.1007/s00500-016-2270-3, 2017.

[6] Zhongda Tian, Shujiang Li, Yanhong Wang, Quan Zhang, "Multi permanent rmagnet synchronous motor synchronization control based on variable universe fuzzy PI method," *Engineering Letters*, vol. 23, no. 3, pp. 180-188, 2015.

[7] Zhongda Tian ,Shujiang Li, Yanhong Wang, "T-S fuzzy neural network predictive control for burning zone temperature in rotary kiln with improved hierarchical genetic algorithm," *Int Journal of Modeling, Identification and Control*, vol. 25, no. 4, pp. 323-334, 2016.

[8] Zhongda Tian, Xianwen Gao, Dehua Wang, "The Application Research of Fuzzy Control with Self-tuning of Scaling Factor in the Energy Saving Control System of Pumping Uni," *Engineering Letters*, vol. 24, no. 2, pp. 187-194, 2016.

[9] Zhongda Tian, "Main steam temperature control based on GA-BP optimized fuzzy neural network," *Inter-national Journal of Engineering Systems Modelling and Simulation*, vol. 9, no. 3, pp. 150-160, 2017.

[10] Yanping Liang, "A kind of novel method of service-aware computing for uncertain mobile applications," *Mathematical and Computer Modelling*, vol. 57, no. 3-4, pp. 344-356, 2013.

[11] Degan Zhang., "A new approach and system for attentive mobile learning based on seamless migration," *Applied Intelligence*, vol. 36, no. 1, pp. 75-89, 2012.

[12] Zhou S, Ya-meng Tang, "A low duty cycle efficient MAC protocol based on self-adaption and predictive strategy," *Mobile Networks & Applications*, 2. DOI: 10.1007/s11036-017-0878-x, 2017.

[13] Xiaodan Zhang, "Design and implementation of

embedded un-interruptible power supply system (EUPSS) for web-based mobile application," *Enterprise Information Systems*, vol. 6, no. 4, pp. 473-489, 2012.
[14] Juntao Gao, Yulong Shen, Xiaohong Jiang, Osamu Takahashi, Norio Shiratori, "End-to-End Delay Modeling for Mobile Ad Hoc Networks. A Quasi-Birth-and-Death Approach," *Ad Hoc & Sensor Wireless Networks*, 2015.
[15] X J Kang, "A novel image de-noising method based on spherical coordinates system," *EURASIP Journal on Advances in Signal Processing*, 2012(110):1-10. DOI:10.1186/1687-6180-2012-110, 2012.
[16] Xiaodong Song, Xiang Wang. "New Agent-based Proactive Migration Method and System for Big Data Environment(BDE)," *Engineering Computations*, vol. 32, no. 8, pp. 2443-2466, 2015.
[17] Xiang Wang, Xiaodong Song. "New Medical Image Fusion Approach with Coding Based on SCD in Wireless Sensor Network," *Journal of Electrical Engineering & Technology*, vol. 10, no. 6, pp. 2384-2392, 2015.
[18] Zhao C P, "A new medium access control protocol based on perceived data reliability and spatial correlation in wireless sensor network," *Computers & Electrical Engineering*, vol. 38, no. 3, pp. 694-702, 2012.
[19] Li W B, "Novel Fusion Computing Method for Bio-Medical Image of WSN Based on Spherical Coordinate," *Journal of Vibro Engineering*, vol. 18, no. 1, pp. 522-538, 2016.
[20] Degan Zhang, Xiang Wang, Xiaodong Song, "A Novel Approach to Mapped Correlation of ID for RFID Anti-collision," *IEEE Transactions on Services Computing*, vol. 7, no. 4, pp. 741-748, 2014.
[21] Ma Z, "A Novel Compressive Sensing Method Based on SVD Sparse Random Measurement Matrix in WSN," *Engineering Computations*, vol. 33, no. 8, pp. 2448-2462, 2016.
[22] Yanan Zhu, "A new constructing approach for a weighted topology of wireless sensor networks based on local-world theory for the Internet of Things (IOT)," *Computers & Mathematics with Applications,* vol. 64, no. 5, pp. 1044-1055, 2012.
[23] Ma Z, "Shadow Detection of Moving Objects Based on Multisource Information in Internet of Things," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 29, no. 3, pp. 649-661, 2017.
[24] Marti, S, Giuli, T. J, Lai, K., Baker, M, "Mitigating routing misbehavior in mobile ad hoc networks," *Mobile Computer Networks*, pp. 255-265, 2000.
[25] Liu, K, Deng, J, Varshney, P. K, Balakrishnan, K, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput*., vol. 6, no. 5, pp. 536-550, 2007.
[26] Elhadi M, Shakshuki, Nan Kang; Tarek R. Sheltami, "EAACK-A Secure Intrusion-Detection, System for MANETs," *IEEE Transactions on Industrial*, vol. 60, no. 3, 2013.
[27] Abdulsalam Basabaa, Tarek Sheltami and Elhadi Shakshuki, "Implementation of A3ACKs intrusion detection system under various mobility speeds," *5th International Conference on Ambient Systems, Networks and Technologies* (*ANT-2014*), Science Direct, Procedia Computer Science 32(2014) 571-578, 2014.
[28] Song X D, Wang X, "Extended AODV Routing Method Based on Distributed Minimum Transmission (DMT) for WSN," *International Journal of Electronics and Communications*, vol. 69, no. 1, pp. 371-381, 2015.
[29] Ke Zheng, Ting Zhang, "A Novel Multicast Routing Method with Minimum Transmission for WSN of Cloud Computing Service," *Soft Computing*, vol. 19, no. 7, pp. 1817-1827, 2015.
[30] Ke Zheng, Dexin Zhao, "Novel Quick Start (QS) Method for Optimization of TCP," *Wireless Networks*, vol. 22, no. 1, pp. 211-222, 2016.
[31] Degan Zhang, Guang Li, Ke Zheng, "An energy-balanced routing method based on forward-aware factor for Wireless Sensor Network," *IEEE Transactions on Industrial Informatic*s, vol. 10, no. 1, pp. 766-773, 2014.

Thanuja. R is an Assistant professor in Computer Science and Engineering Department in SASTRA University. She has published her work in peer reviewed international journals. Her research area includes security issues in MANETs, IDS/IPS design, security in wireless Adhoc Network.

A. Umamakeswari received her doctorate degree from Sastra University, India She is working as an Associate Dean in Computer Science Department, Sastra University. Her research area includes Security in Wireless Sensor Network, Cloud computing, embedded system and IOT. She has published many papers over the last years in high impact journals and conferences proceedings.