Journal of the Nigerian Association of Mathematical Physics
Volume 56 **(March – May** *2020 Issue***), pp47 – 52**
© J. of NAMP

A COLLABORATIVE AND TRUST-BASED SECURE INTRUSION DETECTION SYSTEM FOR MOBILE AD HOC NETWORK

Akinola O.C., Ojesanmi O.A., Onafowora T. and Salako T.

Department of Computer Science, Federal University of Agriculture, Abeokuta.

Abstract

The main objective of intrusion detection system (IDS) is to categorize the normal and suspicious activities in the network. Secure routing established a reliable path between each pair of nodes, while the key management involved is in generation of authentication, digital signature and encryption of information. This paper developed a collaborative and trust-based secure intrusion detection system for mobile ad hoc networks (MANETs). The system used P-coding, a lightweight encryption scheme to provide confidentiality for network-coded MANETs in an energy-efficient way. The trust model works in conjunction with Batman routing protocol to ensure secure route, while the fuzzy inference engine was used to differentiate the trusted node from malicious node. GNS 3 was used to visualize the proposed scenarios and evaluate the performance of the proposed system in mobile ad hoc networks. Simulation results show that the proposed system efficiently detect data traffic attack with high true positive rate and low false positive rate.

I. INTRODUCTION

MANET is autonomous and decentralized wireless systems consist of mobile nodes that are free in moving in and out in the network [1]. In [2], MANET was described as a collection of dynamic wireless mobile nodes which form a temporary network without any fixed infrastructure. They are multi - hop wireless networks. The node uses intermediate nodes to send packet to remote nodes. For this purpose, different distributed routing protocols are required**.** The MANET routing protocols are facing different routing attacks, such as wormhole replay, colluding misrelay attack, flooding, link spoofing, link withholding, blackhole [3]. A large number of attacks have been identified in the recent research that affects routing in ad hoc wireless networks. In [4], attacked are classified into two: Passive and Active attacks. Many researchers have conducted different detection techniques to secure the network. However, existing system architectures are not without criticism, there are still many challenges facing existing scheme. Secure Routing protocols deals with how a node sends message to other nodes or a base station. The goal of a secure routing protocol is to ensure the integrity, authentication, and availability of messages.

Routing protocols in MANET can be classified into two categories: reactive protocol and proactive protocol [5]. Reactive routing protocols for mobile ad hoc networks are also called "on-demand" routing protocols. In a reactive routing protocol, routing paths are searched for when needed. The proactive routing protocols make the fresh list of destinations before the result is required. The route is maintained by routing table i.e. all nodes need to maintain a consistent view of the network topology. Other challenges are highlighted below:

(a) Inability to detect various attacks; hence the need for Hybrid [6]

(b) High resource cost needed for the implementation which makes it not suitable for small and medium level storage users.

(c) Most of the existing work are not in real-time environments; hence, the possibility of data leakages.

(d) Some approaches used Trust. This stands the chance of having a mismatch problem which can occur between the trust requirements and what the designer provided. Also due to the lack of a trusted centralized authority there are lack of trust relationships between mobile nodes [7]

(e) There is a need to create incentive design to discourage dishonesty and reward honesty of MANET participants [8]

(f) Traditional intrusion detection systems (IDSs) work in isolation and are not effective to detect unknown threats [9]

(g) There is need to improve on the acknowledgement and key exchange approach in order to monitor misbehaving node [10].

Based on these major challenges, this paper presents a collaborative and trust-based secure intrusion detection system for mobile ad hoc network.

2. LITERATURE REVIEW

Many research work in securing MANET are still ongoing. In [11], three key aspects to be covered by any security policy on Ad-Hoc networks in order to satisfy the aforementioned security requirements was presented. These are; Intrusion detection-a process of monitoring activities in a system which can be a computer or a network to detect anomalies. Secure routing- establishing a reliable and secure route between each pair of nodes, and Key management service- generation of authentication, digital signature and encryption of information. It was noted in [12] that it is not enough to implement a Key Management Service, it should be accompanied by other two types of solutions. Intrusion detection and prevention mechanism for Mobile Ad Hoc Networks was developed in [13]. In [14], EAACK was designed and implemented with RSA and

Corresponding Author**:** Akinola O., Email: dejioje@yahoo.com, Tel: +2348056052007, +2348034156903

DSA digital signatures using DSR routing protocol. An enhancement of the Watchdog / Pathrater form of Intrusion Detection in Mobile wireless ad-hoc networks (MANET) was designed in [15]. The participating nodes were allowed to listen to the nodes they have conveyed messages to, in promiscuous mode, if within a certain timeframe the message is not relayed, then the node is suggested to be tagged as a misbehaving node. In [16] EAACK was developed with the aim to overcoming the weaknesses in traditional Watchdog mechanism, namely; ambiguous collisions, receiver collisions, limited transmission power and false misbehavior. But there is no authentication for acknowledgements. Composite Trust-based Public Key Management in Mobile Ad Hoc Networks was introduced in [17]. Collaborative intrusion detection networks and insider attacks was designed in [18]. Intrusion detection using fuzzy data mining was introduced in [19]. Fuzzy logic based technique using trust authentication for secure data exchange in wireless sensor networks was the approach used in [20]. The technique established secure links between the nodes in order to guarantee high security, integrity and better performance in wireless sensor network. An IDS which detects and prevents black hole attacks in MANET using cooperative bait detection scheme was designed by [21]. A secure knowledge algorithm in order to detect and mitigate black hole attack on AODV by taking packet drop reasons into consideration was the focus of [22] while [23] introduced adaptive anomaly-based intrusion detection system using fuzzy controller. Majority of these existing work is deficient on the severity of attack, it incurs a low overhead on the network which leads to degradation in network performance.

3. METHODOLOGY

Our research methodology is a collaborative approach on fuzzy trust model for secure routing which comprehensively studies routing attacks and its countermeasures in MANET. Due to the security needs in MANET, integrated leader based IDS used by [24] was replaced by clustered head allowing every node to participate in running its IDS in order to collect and identify possible intrusions. The combined effort of these nodes form a global detection process initiated by clustered head. The clustered head is responsible for detecting intrusions after a predefined period of time. The main challenge is focusing on designing the robust security solution that can protect MANET from various attacks. This work proposes an addition to the routing security suite with the combination of fuzzy trust model with Batman routing algorithm.

3.1. SYSTEM ARCHITECTURE

The system architecture contains four major modules as shown in Figure 1.

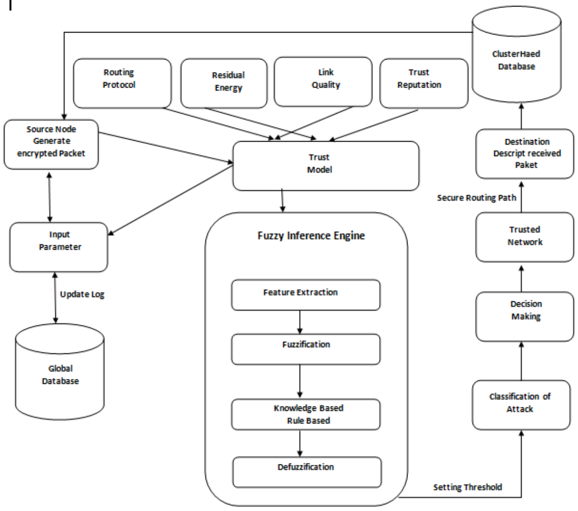

Figure 1: Intrusion detection architecture

(a) Modified Routing Protocol: BATMAN was adapted as the default routing protocol in this dynamic model for the ad-hoc network because of its high performance and low overhead and decentralization of the knowledge through the best route in the network — no single node has all the data. This technique eliminates the need to spread information concerning network changes to every node in the network. The individual node only saves information about the "direction" it received data from and sends its data accordingly. The data gets passed on from node to node and packets get individual, dynamically created routes. A network of collective intelligence was created. This is very important because bandwidth is very limited in wireless communication. The source node first broadcasts a route request (RREQ) message to all adjacent nodes and waits for the corresponding route reply (RREP) message from the destination node to establish routing information. This request and reply query cycle continues as long as this particular path is not listed in the routing table. Once routes have been built from source to destination, they continue to be maintained as long as they are needed by the source node. All wireless packets between these two parties follows the pre-build routing information and forwards node by node until they reach the final destination. When communication ends, the links time out and eventually be removed from the table to release space for other routing paths.

(b) Encryption Modules: P-Coding, a lightweight encryption scheme that provides confidentiality for network-coded MANETs in an energy-efficient way was used. The basic idea of P-Coding is to let the source randomly permute the symbols of each packet (which is prefixed with its coding vector), before performing network coding operations. Without knowing the permutation, eavesdroppers cannot locate coding vectors for correct decoding, and thus cannot obtain any meaningful information. After receiving the encrypted packets, the destination node decrypts the packet by elimination method. We demonstrate that due to its lightweight nature, P-Coding incurs minimal energy consumption compared to other encryption schemes.

(c) Residual Energy: Every transmitted or received packet consumes power. Energy consumption due to transmission is greater than that of reception of packets. So, reliable and active nodes are subject to more power consumption as these nodes are more trusted for packet forwarding compared to their less reliable peers. Therefore, it is found that reliability and residual energy are inversely related to each other. Greater residual energy is one of our criteria for high trust value.

Here, the residual energy is formulated by modified [25]. Let G = (V,E), where each node u ε V is associated with its remaining amount of energy, denoted as β(u). We consider directed edges between nodes because of the possibility for different nodes in consuming different energy in packet transmissions (with different communication ranges). Each directed edge (u, v) ε E is associated with a weight *w* (u, v) to denote the amount of energy needed for a node, u, to transmit one session of data packets to another node v, and a constant (v) denotes the energy consumption of receiving one session of data packets for node v. Note that the transmission of a node by wireless medium can be received by all of the nodes within its communication range. With such a consideration, the *residual energy* of a node, u, over a network, T, rooted at the source, s, is given in equation (1):

$$\hat{\beta}_T(u) = \begin{cases} \beta(u) - \max\limits_{\forall(u,v)\in T}\{\omega(u,v)\} & \text{if } u = s, \\ \beta(u) - \max\limits_{\forall(u,v)\in T}\{\omega(u,v)\} - \gamma(u) & \text{otherwise.} \end{cases} \qquad (1)$$

In equation (1), it implies that each node in T, except malicious node, transmits exactly one session of data packets. Each node in T, except the source node, receives exactly one session of data packets. Source node initiates transfer of data packets, while *malicious node* receives data packets but does not send them to others. Given an ad hoc network, G, our approach choose to find a proper with maximum residual energy to deliver data packets from a source to a set of destinations (reachable from the source). To determine the node with highest residual energy along a path in the network, this is shown in equation (2).

$$\left\{\dot{B}_T(u) \,\middle|\, \forall\, u \in G\right\} \qquad (2)$$

(d) Link Quality Model : Link qualities can be defined as ability of a given link and devices to:
(i) support the density of the traffic for the period of connection,
(ii) be as long as possible stable,
(iii) have less bit errors and;
(iv) reach its destination with the maximum signal strength.

The link state between two neighbors can be affected by many parameters such as distance, battery power and mobility. The second parameter used in route selection is the number of connections over the same path [26]. It is preferred to choose paths with fewer connections (traffic) as route in order to save resources of intermediate nodes, increase the system lifetime as well as the end to end delay over this path. Link quality is usually evaluated according to the received signal strength, because the transmission power of the wireless medium is proportional to the link quality, since a signal with high strength is more stable and has less bit errors. The reception power, LQ, for a signal transmitted with power $\boldsymbol{P_t}$ at a distance ***d*** is given in equation (3):

$LQ = P_t$ x G_r x G_t x $(\lambda^2 /(4\pi d)^2)$ (3)

where
LQ*= received signal strength,*
$\boldsymbol{P_t}$ *= transmitted signal strength,*
$\boldsymbol{G_t}$ *= source node residual energy,*
$\boldsymbol{G_r}$ *= destination node residual energy,*
λ *= wavelength,*
d *= distance.*

From equation (3), evaluating the link quality according to the received signal strength can be descriptive for other network factors such as:
(i) The battery power: this factor is very important since a node with less energy in its battery have small transmission range which affects the quality of links with its neighbourhood. In the other hand, it cannot forward data for a long time. Whenever the battery level is low the transmission power is also low and therefore the reception power is low, thus this link has not high quality.
(ii) The distance: the reception power is relative to the distance between nodes since whenever the distance increase, the link quality decreases.
(iii) The mobility: the link between two nodes is directly affected by nodes' mobility in the way that the link quality decreases whenever neighbours are going away from each other and increases whenever they go closer.

Trust Model: This section discusses the trust unit which works in conjunction with BATMAN routing protocol. Route cache will be maintained from where the route selector can choose a route whose trust has to be evaluated. The model is built with the intentions of making a trusted network for secure routing. The model is divided into four different unit with each unit designated a particular task.
(i) Unit A: Manages all the trust modules and helps in coordinating among all the trust evaluating modules.
(ii) Unit B: Stores information about all the current active routes from source to destination..
(iii) Unit C: Helps in building the trust among the nodes and finally in forming the trust of a route.
(iv) Unit D: This unit stores the current trust value of a route and periodically compares the new evaluated value of the route with the stored value and if a new trust value is found , it updates it.

Trust value of a node depends on the number of packets it has successfully transmitted. A node sends a positive or negative acknowledgement based on successful or unsuccessful transmissions respectively. Acknowledge monitor keeps a track of these acknowledgements and uses it as experience for evaluating new trust value and also select the most reliable route from source to destination depending on the trust level.

(i)Trust Updating Policies: Assume each node's opinion towards one another initially is (0, 0, 1) which means total uncertainty. Suppose node, A, wants to discover a routing path to B. Because the uncertainty element in A's opinion towards others is larger than or equal to 0.5, which means that A is not sure whether it should believe or disbelieve any other nodes. A will use the P-coding schemes to perform routing discovery operations. After some successful or failed communications, A will change its opinions about other nodes gradually using the trust updating algorithm. The uncertainty elements in its opinions about other nodes will be mostly less than 0.5 after a period of time. By means of this procedure, eventually each node in the network will form more certain opinions towards other nodes eventually after the initial time period.

Once the trust relationship is established among most of the nodes in the network, these nodes can rely on our trusted routing protocol which is based our trust model to perform routing operations. Node A now will utilize the trust recommendation protocol to exchange trust information about a node, B, from its neighbours, then use the trust combination algorithm to combine all the recommendation opinions together and calculate a new option towards B. The subsequent routing discovery and maintenance operations will follow the specifications of our trusted routing protocol.

(ii) Trust Mathematical Model: This section gives the mathematical formulation of the system which helps in choosing the most reliable route from source to destination. When a node joins the network an initial trust level is assigned to the node to be the part of the network. With this initial trust value node is allowed to participate in all the transmissions. Based on the successful and unsuccessful transmissions done by a node its new trust value is evaluated. The new trust level of a node can be calculated using equation (4). The combine model of [27] was used to calculate Trust level and Forward Packet Ratio as stated thus:

Consider a MANET of N node. Suppose $n \epsilon N$

where

N → is set of all nodes in a route from source to destination.

n → is a node in a route from source to destination.

$${}_{n}G_{new} = 0.95*({}_{n}G_{o})+0.05*({}_{n}G_{E}) \qquad (4)$$

where

${}_{n}G_{new}$ → new trust level of a node *n*

${}_{n}G_{o}$ → Old trust level of a node *n*

${}_{n}G_{E}$ → trust level of node *n* based on experience (acknowledgement)

Let G = (V,E), where V = $\{v_1, v_2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots v_n\}$ and E = $\{e_1, e_2, \ldots\ldots\ldots e_n\}$

The reputation is stated in equation (5):

$${}_{n}G_{t} = \begin{cases} +t & \text{Positive Acknowledgement (PA)} \\ -t & \text{Negative Acknowledgement (NA)} \end{cases} \qquad (5)$$

a link has capacity of carrying one packet per unit i.e. y (e).

When a source wants to send series of packet.

Let X= $\{x_1, x_2,\ldots,x_s\}$to a set of sink S where, where S $\subseteq$ H, then source computes y(e) as shown in equation (6)

$$y(e) = \sum_{e\in(-h)}^{t=h} \beta(e)y(e) \qquad (6)$$

where, β(e) is a Local Encoding Vector(LEV)

Global Encoding Vector can be appended to message

Source encrypts packet with permutation encryption shown in equation (7),

$$C[y(e)] = \sum\nolimits_{e\in(-h)} \beta(e)C[y(e)] \qquad (7)$$

$$Y = GX \qquad (8)$$

Intermediate node forward packet to sink node with simple recoding with no extra efforts.

Sink node will decrypt the packet as shown in equation (9),

$$D\{c[y(e)]\} = E^{-1}\{E[y(e)]\} = y(e) \qquad (9)$$

Thus source packets recover by applying Gaussian elimination,

X= Forward Packet Ratio = G-1(Y)

Hence, FPR = G – 1(GX) (10)

Fuzzy Parameter Extraction:

Fuzzy logic is a form of many-valued logic or probabilistic logic; it deals with reasoning that is approximate rather than fixed and exact. A fuzzy inference system (FIS) is the process of formulating the mapping from a given input to an output using fuzzy logic. The mapping then provides a basis from which decisions can be made, or patterns discerned. In the proposed protocol, Trust value, link quality and residual energy were used for Fuzzy inference engine calculation. The trust of a node is based on Forward Packet Ratio (ratio of packets forwarded to packet received by the node concerned), Residual Energy and Link Quality. The absolute value of each of these parameters can take a large range at different points on the network. We have considered the normalized values for each parameter.

We use a fuzzy-based approach to evaluate the trust of a node and then decide the trustworthiness of a node. Consideration has been given to misbehaving nodes and routing attack, while the trust modules chooses the most trusted and reliable route from source to destination and it is achieved by choosing the route with the highest trust level out of all the discovered routes from source to destination. The fuzzy inference engine module is used for detection and likely prediction of future attacks.

Fuzzy Application Model:

Our application of Fuzzy Logic has the following form:

If **condition** *then* **consequence**

where,

Condition is a fuzzy variable.

Consequence is the fuzzy set.

If Forward Packet Ratio, Link quality and Residual energy is **HIGH**
then Attack Rate is Low.
Hence, for every element, *a,* in the set of *A*, there is a mapping a I→μ(a) in which μ(a) ε [0,1]. The set Δ = {(aμ(a))}is defined a fuzzy set for trust in MANETs. μ(a) is defined as the membership function for every *a* in Δ. A membership function defines the degree to which a fuzzy variable is a member of a set. Full membership is represented by 1 and no membership by 0.

3.3. Fuzzy Inference Rules

When node **a** want to transfer packet to node **b**, node, ***a,*** has the difficulty to evaluate whether node ***b*** can utilize the packet at that time or whether the packet sent by node **b** is secure and trustworthy. Then, this situation can be judged and monitored by node *a* from the history interaction records of node ***b***.
Let Forward Packet Ratio (FPR) represent ratio of packets forwarded to packet received by the node concerned, let Residual Energy (RE) represents residual energy of destination node (node b) on providing packets transfer services at time ***t***. Let Link Quality (LQ)*)* represents link ratio between the past time intervals. Let *Attack Rate (AR)* refers to the outcome of three aforementioned parameter at time *t+1*. The function of the Fuzzy inference engine and method by which the outputs of each rule are combined to generate the fuzzy decision are (R represents rule):-

R1:- If FPR is very low and RE is very low and LQ is very low, then AR is very low.
R2:- If FPR is low and RE is very low and LQ is very low, then AR is very low.
R3:- If FPR is average and RE is very low and LQ is very low, then AR is very low.
R4:- If FPR is high and RE is very low and LQ is very low, then AR is very low.
R5:- If FPR is very high and RE is very low and LQ is very low, then AR is very low.
R6:- If FPR is very low and RE is low and LQ is very low, then AR is very low.
R7:- If FPR is low and RE is low and LQ is very low, then AR is low.
R8:- If FPR is average and RE is low and LQ is very low, then AR is low.
R9:- If FPR is very high and RE is low and LQ is very low, then AR is average.
R10:- If FPR is very low and RE is average and LQ is very average, then AR is very low.
R11:- If FPR is low and RE is average and LQ is very average, then AR is low.
R12:- If FPR is average and RE is average and LQ is very average, then AR is average.
R13:- If FPR is high and RE is average and LQ is very average, then AR is average.
R14:- If FPR is very high and RE is average and LQ is very average, then AR is high.
R15:- If FPR is very low and RE is high and LQ is very high, then AR is very low.
R16:- If FPR is low and RE is high and LQ is very high, then AR is low.
R17:- If FPR is average and RE is high and LQ is very high, then AR is average.
R18:- If FPR is high and RE is high and LQ is very high, then AR is high.
R19:- If FPR is very high and RE is high and LQ is very high, then AR is high.
R20:- If FPR is very low and RE is very high and LQ is very high, then AR is very low.
R21:- If FPR is low and RE is very high and LQ is very high, then AR is low.
R22:- If FPR is average and RE is very high and LQ is very high, then AR is average.
R23:- If FPR is high and RE is very high and LQ is very high, then AR is low.
R24:- If FPR is very high and RE is very high and LQ is very high, then AR is very low
According to these inference rules stated above, we got the output as crisp values (i.e. an attack of non-attack)

3.4 Intrusion Response

The majority of intrusion response systems (IRSs) react to attacks by generating reports or alarms. The responsibility to take an effective action is left to the system administrators. This introduces a window of vulnerability between when an intrusion is detected and when action is taken to defend against the attack. An appropriate response for an intrusion attempt is determined by two conditions – firstly, how much you trust the host who is claiming to be a victim and secondly, how suspicious are you of the alleged attacker. We use two parameters to form the heuristics, *Trust Level* and *Suspicion Rank,* which correspond to the two conditions.
Trust Level is determined by the extent to which the node is convinced from its own logs about the attack claimed by the victim. This value is incremented if the attack is successfully proved and reduced if the proof fails. The reduction in the level of trust on a failed proof would discourage false attack claims, possibly from an attacker masquerading as a victim. The Mobile agent will initiate the response and transporting packet.

3.5 Implementation and Evaluation

GNS 3 package is used for the simulation to provide multiple solutions for managing networks and application network operation, planning and performance management. The metrics for evaluating the performance of the model are:
Packet delivery ratio are used to define the performance of network. PDR defines the ratio of the number of packets standard by the destination node to the Number of packets sent by the source node.
Routing overhead: RO defines the ratio of the amount of routing-related transmissions [Route Request (RREQ), Route Reply (RREP), Route ERRor (RERR).
Total energy consumption: Total amount of energy consumed by each node in the network.
Average Latency. It is defined as the mean time in seconds taken by the data packets to reach their respective destinations.
Throughput. Defined as the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet.
Round-Trip-Time is the time required for a single packet to travel from a specific source to destination and back again.
Window Size is the number of data packets that can be sent without waiting for an acknowledgement. Window Size = Throughput * RTT

4.0 Conclusion

The security issues in MANET has been in perspective and preventive based methods such as encryption and authentications have not eliminated attacks, hence a collaborative and trust based secure intrusion detection system was developed combining routing security suite with fuzzy trust model with BATMAN routing algorithm. Major parameters such as packet delivery ratio, routing overhead, total energy consumption, average latency, throughput, round-trip-time and window size were used to test the performance of the model. The proposed scheme improves the network performance when properly deployed.

REFERENCES

[1] Baberwal D. and Mahesh B. (2015), “Detection and Prevention of Black Hole Attack for Dynamic Source Routing in Mobile ad-hoc Network”, International Journal of Innovations & Advancement in Computer Science, ISSN 2347 – 8616 Volume 4.

[2] Deepika K. and Poonam V. (2015) “Routing Protocols for MANET, VANET and AANET”: A Survey, International Journal of Innovative Technology and Research, Volume No.3, Issue No.2.

[3] Nadeem A. and Michael H. (2013),"Protection of MANETs from a range of attacks using an intrusion detection and prevention system”, "Telecommunication Systems 52(4), pp. 2047-2058.

[4] Raja L. and Santhosh B. (2014) “An Overview of MANET: Applications, Attacks and Challenges” International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1.

[5] Kumar P. K. and Rama V. V. (2015) “Efficient Ant Colony Optimization (ACO) based Routing Algorithm for Manets”, Global Journal of Computer Science and Technology: E Network, Web & Security, Volume 15, Issue 3.

[6] Dina S.J and Shahrbanoonezhad A. (2014) “ A Novel Method Intrusion Detection Based on Sending and Checking Packet for Neighbored Nodes in MANET”, Universal Journal of Communications and Network 2(1): 10-13.

[7] Kaur A. and Singh P.T (2015), “Securing MANET from jellyfish attack using selective node participation approach, International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-4.

[8] Murali G, Sivaram R, Prasad K, Bhaskar V, and Rao O. (2015) “Secure Leader Election for Intrusion Detection in MANET”, Department of Computer Science Engineering, Acharya Nagarjuna University, AP, India.

[9] Fung C. J., Zhang J., Aib I., and Boutaba R. (2011). Dirichlet-based trust management for effective collaborative intrusion detection networks. Network and Service Management, IEEE Transactions on, 8(2), pp 79 –91.

[10] Patolial S. B. and Kumar B.N. (2015), “KEAM- To Isolate and Prevent Selective Packet Drop Attack in MANET, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 5.

[11] Yan Z., Zhang P., and Virtanen (2003) “Trust Evaluation Based Security Solution in Ad Hoc Networks”, in The Seventh Nordic Workshop on Secure IT Systems, Norway

[12] Kumar K.Y and Bhavani S. (2015), “Effective Authentication routing scheme for data integrity in MANET”, International Journal of Soft Computing, Vol. 10, No 6, pp. 408-414.

[13] Nadeem A, (2010) ”Intrusion Detection & Prevention Mechanism for Mobile Ad Hoc Networks” Centre for Communication System Research, Faculty of Electronics and Physical Sciences, University of Surrey Guildford, Surrey GU2 7XR, UK.

[14] Sheltami R., Shakshuki, M and Nan K. (2013) EAACK- A Secure Intrusion Detection System for MANETs. IEEE Transactions on Mobile computing, 60(3):1089-1098.

[15] Obimbo C., and Arboleda-Cobo M. (2011), “An Intrusion Detection System for MANET”, IJCSNS International Journal of Computer 258 Science and Network Security, Vol.11, No.5.

[16] Kang N, Shakshuki E. and Sheltami T. (2010), “Detecting Misbehaving Nodes in MANETs”. The 12th International Conference on Information Integration and Webbased Applications & Services (WAS2010), ACM, pp. 216-222.

[17] Cho J. H. and Chan K.S. (2010), “Composite Trust-based Public Key Management in Mobile Ad Hoc Networks”, U.S. Army Research Laboratory 2800 Powder Mill Rd. Adelphi, MD 20783, USA.

[18] Fung C. J. and Boutaba R. (2013). Design and management of collaborative intrusion detection networks. In 15th IFIP/IEEE Intl. Symposium on Integrated Network Management,

[19] Dhopte S. and Chaudhar M. (2014), “Intrusion Detection using Fuzzy Data Mining” International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, pp. 1231-1237.

[20] Blessey P. and Geetha R. (2015) “Fuzzy Logic Based Technique Using Trust Authentication for a Secure Data Exchange in Wireless Sensor Networks, International Journal of P2P Network Trends and Technology (IJPTT), 5(3):5-11.

[21] Agalya N. C. and Sridevi S. (2015) “Detecting and Preventing Black Hole Attacks in MANET using CBDS (Cooperative Bait Detection Scheme)” International Journal of Modern Trends in Engineering and Research (IJMTER) Volume 02, Issue 04.

[22] Siddiqua *et al* (2015). “Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm”, International Conference on , pp. 421-425.

[23] Geramiraz F., Memaripour A. S. and Abbaspour M. (2011), “Adaptive anomaly-based intrusion detection system using fuzzy controller”, International Journal of Network Security, Vol 14, No 6, pp. 352-361.

[24] Devi V. B. and Priya S. (2015) “Intrusion Detection and Response System in MANET Using Leader Election Based Mechanism Design Approach”, International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 9.

[25] Hisham A. K , Fabrizio B, Salim H, Esraa H., Ahmed M. Y and Sahar A. S (2012) “A Hierarchical Intrusion Detection System for clouds: Design and Evaluation “, International Journal on Cloud Computing: Services & Architecture; Vol. 2 Issue 6, p1

[26] Somayeh K. and Reza A. (2015) ”Presentation of Intrusion detection system for MANET networks Based on clustering”, Department of computer engineering, College of Engineering, Qom Branch, Islamic Azad University, Qom, Iran.

[27] Korad, S., Kadam, S., Deore, P., Jadhav, M. and Patil, R. (2016) Detection of Distributed Denial of Service Attack with Hadoop on Live Network. International Journal of Innovative Research in Computer and Communication Engineering, 4, 92-98.