A Secure & Hybrid Authentication Protocol of Intrusion Detection System for MANET

M.CHARLES AROCKIARAJ [1], DR.P.MAYILVAHANAN [2]

[1]Research Scholar, Vels University,Chennai. 600117, mcharles2008@gmail.com
[2]HOD,Dept.of MCA, Vels University,Chennai-600117,Tamil Nadu,INDIA.

Abstract-In MANET, security is the toughest and very challenging area, because nodes are without any predefined framework. This is due to the high mobility of outstanding vulnerabilities and attacks of the malicious nodes in the intrusion detection system of Mobile Ad Hoc Networks (MANET). A secure & hybrid protocol design has been proposed, in order to improve the detection efficiency and also to improvise the performance of Intrusion Detection Systems for MANET. Based on the hybrid techniques with the aid of key management authentication and combining with a fuzzy based decision model for detecting the misbehaving attacks. Identifying group of physical attacker and finding its probabilities and its side effects are evaluated. To discover the misbehaving attackers and predicting it effects by using Fuzzy based model. In the proposed hybrid authentication protocol for malicious node detection system and for avoiding problems related to missing packet, delay in the nodes and false misbehavior reports. Secure hybrid authentication protocol is used to detect various attacks in MANETs by incorporating hybrid techniques such as fuzzy schemes and key organization method. Hence the different ratio of all the parameter were experimented and analyzed, in terms of the attack prediction rate, attack precision, packet drop ratio and end to end delivery ratio. The schemes were compared with the existing mechanisms and results show that proposed hybrid authentication has superior improvement in the performance.

Key Words: Trust Certificate Authority (TCA), Network Trust Administrator Server (NTAS), Fuzzy Model, Predicting Attacker, Packet Loss.

I. INTRODUCTION

MANET is a growing technology, which enable users to communicate without any physical infrastructure, regardless of their geographical location [2]. Hence, it is referred as an infrastructure less network [3]. In MANET, each node acts as the node and a router. Thus the message routing is a problem in a decentralized environment where the topology fluctuates. MANET has various drawbacks like limited bandwidth, battery power, computing power and security [1]. Mobile Ad Hoc Networks (MANETs) need more physical foundation and federal control over the movable nodes. In this type of system, the hub itself assumes the parts of router, server and customer. Moreover nodes are about to execute, benevolently roles to ensure an accurate system performance [4]. All parameters are considered when a hub may get into mischief and neglect to coordinate, due to its overload, broken or because of selfish and even malevolent conduct [2].

In MANETs, message between two hubs that are outer range of transmission extent, so it needs multi-hops path that incorporates moderator nodes for forwarding the data [1]. These moderator nodes are self-sufficient and doubtlessly possibility to turn into an invader node [3, 4]. These invader nodes are performed on UDP based MANETs and their invader technique alters the first uniqueness information of correspondence methodology, making these invader nodes noticeable and consequently, it is simple to find affected nodes [2]. MANETs are more vulnerable against invader nodes due to its absence of main factors such as authority verification, necessity of shared trust based correspondence (i.e., multihop correspondence), dynamic topology and restricted assets. It is hard to actualize a countermeasure calculation productively because of low handling force and battery life [5]. In this paper, it overcomes existing problem by proposing secure and hybrid authentication protocol for identifying the invader node and the primary issue concerned in this assembly with the detection of the Trusted Certificate Authority (TCA) [14]. The issues such as invader nodes in the TCA are overcome by detecting the selfish as well as misbehavior nodes. This assembly does not require TCA, which reveals that it is more adaptable. It needs sufficient time to assemble all the certificate exchange between the systems, because of that reason, the transmitting of crypt coding to the moving clients in a periodical way [6]. The proposed algorithm comprises of the organizer hub, servers and common movable hubs. The organizer nodes act as a middle person for transmitting the packet among the servers and movable hubs. Every node creates its own open/private key sets utilizing server-marked open keying system. The organizer node helps in producing the freely recoverable open key for any nodeN_i without the information of the consequent private key [9]. The facilitator node goes about as a circulated trusted authority certificate power. It joins the shares of (t+ 1) servers for registering mark parameter. The nodes in the systems are accepted by utilizing the trust administration component. The trust certificate is figured by utilizing the Eigen Vector Character Centrality [7]. In the next part of the algorithm, fuzzy based decision model is proposed in this framework to predict the misbehavior nodes and find its prediction ratio and also its occurrence in the nodes [8]. Predicting various invader nodes and also finding possibilities packet drop in the node. The proposed work is to have a secure key organization and also to predict the attacker's occurrence in order to identify the misbehavior nodes and with various possibility parameters were evaluated.

The rest of the paper is organized as: section II deals with literature survey of previous methods and its demerits, section III gives the detailed explanation of proposed secure & hybrid authentication protocol and its methodologies and section IV elaborates about the performance evaluation of the stimulation results and finally section V discuss about the conclusion of the paper.

II. LITERATURE SURVEY

A great deal of studies has been carried out on security prevention measures for infrastructure-based wireless networks. However, few works has been carried out on the possibility of intrusion detection [1]. A. Mishra stressed the challenge for intrusion detection in ad-hoc network and the use of anomaly detection, but didn't give a solution or implementation for the problem. In Huang [7] detailed an anomaly detection technique that investigates the connections features of nodes and discusses about the routing anomalies. Loo [9] presented an intrusion detection method utilizing a clustering algorithm for routing attacks in the sensor networks. It has the capacity to identify three vital sorts of routing attacks. They find themselves able to distinguish sink opening assaults viably which are an exceptional manifestation of assault. There are able to detect sink hole attacks effectively, which are intense form of attack [10]. There are some defects like absence of the simulation platform that supports for a wider variety of attacks on larger networks. Fixed width clustering algorithm has shown to be highly effective for anomaly detection in the network intrusion [8]. It presented a geometric framework for unsupervised anomaly detection. In Mobile ah doc network security, the primary objective was to maintain the secure and abundant information transmission between both the end locations. For the system to perform productively, it is basic to devise a security management that can make the system versatile against different invader in adaptive intrusion detection. Over the recent years, invader has adventure over MANET's vulnerabilities have been proposed in conjunction with conceivable countermeasures [21]. To make the trusted system access instrument more practicable, scientists proposed diverse arrangements that centered on TNC construction modeling. Jungbauer and Pohlmann [15] proposed a strategy to focus the reliability of endpoints which served as a premise for Trust Dependable Correspondence. The model did not oblige particular equipment, for example, TPM (Trusted Platform Module) then again extraordinary working framework structure. Rehbock and Hunt [14] proposed a protocol stack that empowered the utilization of TNC in the web based environment and changed the TNC structural engineering to provide an extra security.

In signature based detection proposed e-TCP, enhanced performance of TCP, to eliminate the impacts of late response of higher difference by Jelly- Fish invader node [16]. Moreover, execution for other assault variations has not been taken into account. A summarizing review on misbehavior hub conduct discovery was given in the self key managements [11]. A reorder thickness based discovery mechanism for identifying jellyfish reorder assaults has been exhibited in countermeasure in TCP-based MANET [12]. Every hub computes the reorder thickness by recording the reordering recurrence of its neighbor hubs. Author, on the other hand, did not give any countermeasure system and no results, simulations or something else, have been displayed to demonstrate the effectiveness of their proposed location strategy. In secure on-demand routing protocol for ad hoc networks [15], scientific model for finding reordering invader by including two new move states in TCP-New Reno was proposed. The Jellyfish dropping attack alongside the black hole invader was mentioned briefly in Purohit et al. [13] without giving any answer for its recognition or anticipation. A shared countermeasure, frequently utilized as premise for other identification strategies was proposed the routing security in the ad hoc wireless networks. Here, the author indicated a hub malicious behavior has found and its identification component called "watch dog" in which a gathering of hubs and its used to monitor other hubs' conduct and rate them consequently [19]. An alternate strategy called "pathrater" was utilized for avoiding the irritating nodes and detected by the watchdogs from making further correspondence action.

The fuzzy set theory and reputation model with this consideration Luo and Fan [9] proposed a subjective trust management model based on certainty-factor for MANETs (CFS trust), which was utilized in quantifying and evaluating the nodes credibility. In their model, the problem of trust management is modeled by fuzzy likelihood estimation and confidence estimation [3]. Particularly in as fuzzy logic classifier, it has been considered that utilization of a vigorous FRBCS, i.e. the Fuzzy logic Association Rule-based Classification for High-Dimensional issues (FARC-HD) [7]. The innermost method of this methodology included an improvement stage for Evolutionary fuzzy logic algorithm [16]. This kind of hybridization is known as Genetic Fuzzy logic System (GFLS) [4, 5]. At last, multi-Purpose GFS have been deeply analyzed in the setting of IDS. In Tsang et al. (2007) the creators propose MPGFIDS (short for Multi-purpose Genetic Fuzzy Intrusion Detection System), which was focused around the past work of the creators related to an Agent based transformative methodology for fuzzy standards [18]. This methodology was focused around the accuracy and prediction advancement, in a Pittsburgh style, of a precise and interpretable fuzzy learning base.

III. SECURE & HYBRID AUTHENTICATION PROTOCOL

The cross layer intrusion detection systems have been implemented with a hybrid scheme of the Key organization authentication and Fuzzy logic based predicted methodology to identify the various misbehavior attackers. The proposed hybrid scheme aims to observe the nodes activity, to predict the misbehaving nodes, to identify the packet drop ratio and estimating the parameters such as possibilities attacker ratio, packets dropping, possibilities of affected packets due to misbehavior nodes performance in the nodes. Thus, the hybrid protocol is used to find the packet loss because of limited power battery or malfunction. Moreover, discovering the misbehaving nodes and to predict its symptoms also calculated in the Fuzzy logic function [3].

The proposed secure hybrid authentication protocol consists of organizer node, servers and typical movable nodes. One organizer node is selected for the Trusted Authority Authentication. The proposed protocol design is made up of Self Trusted key administration method of the MANET. It incorporates the common nodes $(N_1, N_2, ..., N_{10})$, for example, $N_4$is picked as the organizer node (N_o). There are number of n servers denoted as $\{Z_1, Z_2, ..., Z_n\}$. The organizer node always stands as middleperson nodes for transmitting messages from typical movable nodes to the servers. Thus the Proposed Secure & Hybrid Authentication Protocol involves an eight steps process:

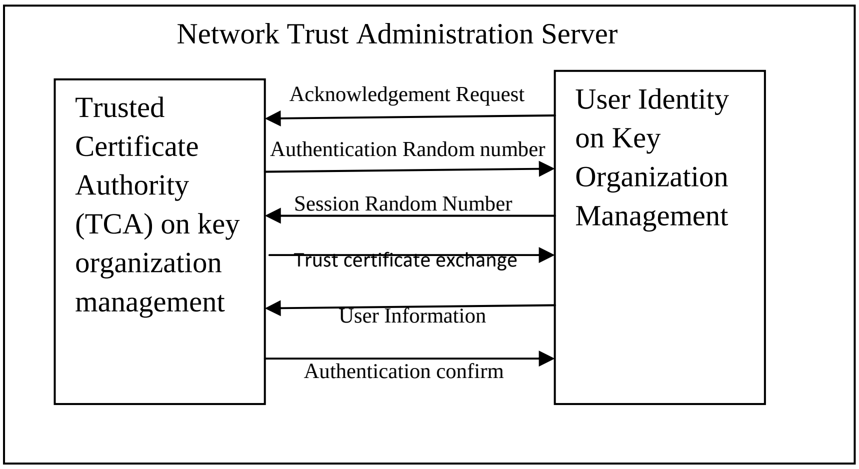
A. *Steps for Process of Hybrid Authentication Protocol:*

- Criteria in Trusted Certificate Authority
- Authentication on Network Trust Administration server
- Predicting the Misbehavior nodes
- Path Determination
- Predicting the Possibilities of the Packet Drop
- Predicting the Possibilities of Loss Packet
- Predicting Attack Precision
- Predicting end to end delivery ratio

Thus the security and higher precision to predict the misbehavior node is enhanced by using the hybrid authentication protocol

a. Criteria in Trusted Certificate Authority

It is a major part of Network security, in which a Trusted Certificate Authority (TCA) is incorporated and the organizer node N_o ends the request (R) sends the metric data to the Authentication Trust administration server where it needs to be a part of the system [3]. The trust administration component is utilized to accept the hubs in the system. The trust based value utilized for Eigen Vector character Centrality. Every hub send in the system blocks, the Eigen Vector Centrality (EVC_i) of its neighbors for showing the higher level of authentication on each neighbor [5].


Network Trust Administration Server
Trusted Certificate Authority (TCA) on key organization management
User Identity on Key Organization Management
Acknowledgement Request
Authentication Random number
Session Random Number
Trust certificate exchange
User Information
Authentication confirm

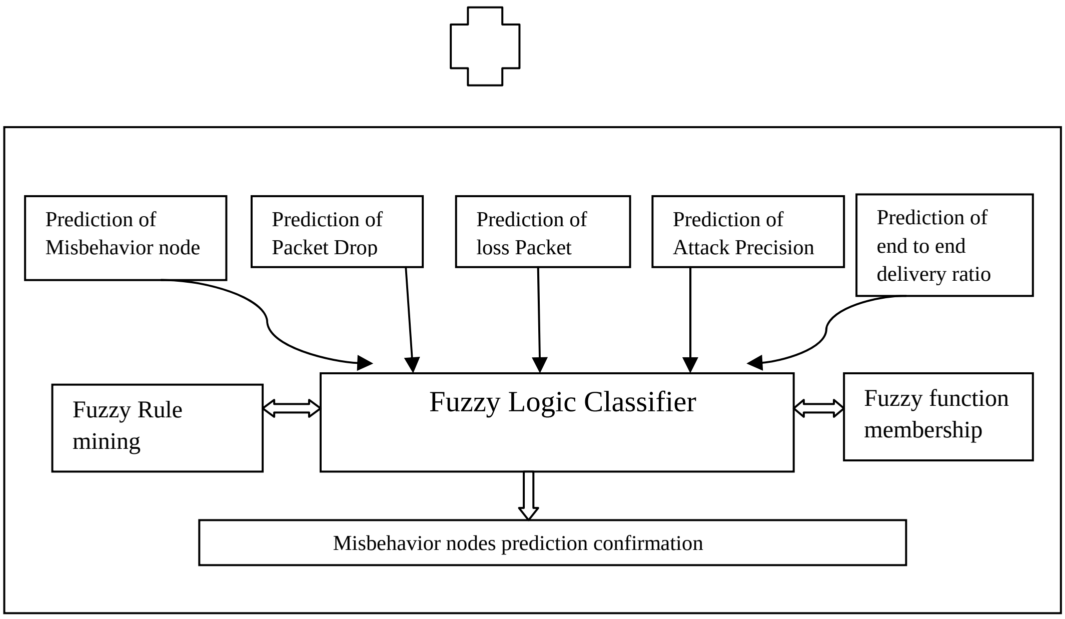

Prediction of Misbehavior node
Prediction of Packet Drop
Prediction of loss Packet
Prediction of Attack Precision
Prediction of end to end delivery ratio
Fuzzy Rule mining
Fuzzy Logic Classifier
Fuzzy function membership
Misbehavior nodes prediction confirmation

Figure 1: The Architecture Diagram for Secure & Hybrid Authentication Protocol

In hybrid authentication protocol, the user identify in network trust administration server sends request to the trusted certificate authority server, as demonstrated in the architecture diagram and that user sends acknowledgement for data collection, programming data, current framework details and open key of R to the trusted organization server. The Network server confirms the information. In case it is right, the server will produce a trust value to the user.

b. Authentication on Network Trust Administration Server (NTAS)

Authentication of ACK and Ack0, where their methodology Ids are user ack1 and user ack2, respectively by utilizing network trust administration Part server

(N_o , NTNS: open key, data information, Rcv: channel (dy))

Accessed by Organizer node
init State:=0
Move:

State0:=2/n request (N_o , NTNS, acknowledgement REQ1)

State0:=4/n request (N_o , NTNS, acknowledgement REQ12)

It implies that organizer node N_o appeals to check both ACK and Ack0. In case, if authentication is positive then N_o acquire a recognized message.

The organizer node hub circulates as a circulated trusted certificate power. It joins the shares of (t+ 1) servers for registering the marked parameter. Consider that the organizer hub chooses the primes x, λ with $\lambda \mid x-1$, an originator d of a multiple sub groups on the key organization system of Z_x^* with request λ. Let h (.) indicates a hash capacity and N_i indicates any node in the system. The organizer node distributes x, λ, d and h and the trusted certificate authority will generate the authentication random number $K'_{Ni} \in_R Z\lambda^*$ and organizer nodes produces private value to user identify on key management by computing $O'_{Ni} = d^{(K'Ni)}$. Network Authentication (needs session key). The organizer node sends a user verification appeal to NTAS. The acknowledgement incorporates Authentication Random Number (ARN- id), username (user-id), and the Current Session Identifier (CSI). Organizer sends the acknowledgement marked by N_o^{-1} to NTAS.

$$N_o \rightarrow NTAS:\{CSI \,||\, ARN_{id} \,||\, User_{id}\}N_0^{-1} \tag{1}$$

NTMS produces and sends a session key arbitrary number to organizer node N_o . NTMS produces and forwards the current session identifier, if the user authentication is confirmed through its authentication random number (ARN-id) and user -id. NTMS produces a session key arbitrary number $Nonce_{NTAS-CSI}$ and encodes it by User open key. NTMS signs the cryptograph (CSI) and then sends user data to the organizer node.

$$NTAS \rightarrow N_o : \{Nonce_{NTAS-CSI} \,||\, N_o(openKey) \,||\, CSI\}NTAS^{-1} \tag{2}$$

The organizer node T_{AVC} send the user information to the network trusted administration server and N_o decrypts CSI by the open key of NTMS and the Authentication Random number $Nonce_{NTMS-SI}$ utilizing its own particular secret key. At that point, N_o produces another session random number $Nonce_{NTAS-SI}$ and with message validation codes C_{MVC}, which assure data collection trust value. N_o Uses the pseudo-Authentication Random number (PARN) to predict the session Identifier (SI) by utilizing the $Nonce_{N_o-SI}$, C_{MVC} and the current session identifier CSI. SI's figuring out mathematical statement is

$$SI = PARN(Nonce_{NTAS-SI}, Nonce_{N_o-SI}, CSI) \tag{3}$$

N_o Encodes the username U_{id}, user secret id S_{id}, and in the Network Trust Administration Server (NTAS) to get the Trusted Certificate Authority value confirmation in the key management T_{AVC} to SI. N_o's secret key validated in Trust value key management, $\{Nonce_{SI}\}, nonce_{NTAS-SI}$, CSI and C_{MVC}, sends this user information data to NTAS.

$$N_o \rightarrow NTAS : \{\{Nonce_{N_o-SI} \,||\, NTAS_{(openkey)} \,||\, CSI \,||\, C_{MVC} \,||\, U_{id} \,||\, S_{id} \,||\, T_{AVC}\}SI\}N_o^{-1} \tag{4}$$

NTAS sends back acknowledgement authentication to the organizer node N_o. $NTAS^{-1}$ Decodes { $Nonce_{N_o-SI}$ } $NTAS_{(openkey)}$. NTAS gets the Authentication random number $Nonce_{N_o-SI}$. NTAS formulates the session Identifier SI utilizing the two current session identifier random number and the current session identifier CSI. At that point { $U_{id} \,||\, S_{id} \,||\, T_{AVC}$ } SI is decoded by the session key SI. NTAS can acquires the user id and secret id, analyzes the user data information in NTAS. In case the user identifier is right, NTAS sends Acknowledgement confirmation to the organizer node N_o and permits the organizer node N_o to get to the Trust Certificate Authority value by the TCA in the NTAS. The Authentication Pass methodology is finished with the accompanying activity:

$$NTAS \rightarrow N_o : \{\{ACK_{Pass}\}SI\}NTAS^{-1} \tag{5}$$

c. Prediction of Misbehavior nodes

The organizer node N_o gathering information about the trust certificate authority value for all node as well as predicting overall possible gateway to the nodes. The organizer node N_o in the Network Trust Administration Server, gathers the trust certificate authority value $T_{CAV} > T_{CAV_{\min}}$, of the nodes are considered in the overall possible ways. $T_{CAV_{\min}}$ Depends on the minimum trusted value from the Trusted certificate Authority in the NTAS. The minimum trust value replies upon the overall possible nodes in the Network Trusted Administration Server (NTAS) of the system. The common nodes must have a Trust Certificate Authority Value T_{CAV}, higher than the minimum trusted value $T_{CAV_{\min}}$, of the Network Trusted Administration Server (NTAS) of the system.

$$T_{CAV} > T_{CAV_{\min}} \tag{6}$$

Thus by calculating minimum trusted value, if the nodes have lesser than $T_{CAV_{\min}}$ value then it is easy to predict the misbehavior node in the server.

d. Path Determination

Among the acquired ways, organizer node N_o chooses a way such that it has more secure and certified path to the final destination node .Once after the path have been selected the gateway, organizer node N_o and user identify checks the trusted certificate authority value and open key also and then only set the determined path between each other.

e. Predicting the Possibilities of the Packet Drop

The fuzzy based prediction model is used for identifying misbehavior nodes in MANET. In this proposed method, it is observe the movement of nodes and including parameters, such as prediction of packet dropping, prediction of lost packets, prediction of attacker precision and prediction of end to end delivery ratio because of depleted battery influence or glitch. For every node in the network trust administration server is used for predicting the symptoms of the misbehavior node are also formulated. For fuzzy based prediction model it calculates the prediction and trust value for all the parameter.

Let N_{E_i} and $N_{E_{res}}$ be the initial node and residual energy of the node.

Let β be the average lifetime of the nodes in the server.

Let $T_{CAV_{\min}}$ be the minimum trusted certificate authority value of misbehavior node.

Let $P_{PD} = \frac{1}{T_{CAV_{\min}}}$ be the threshold values of predicting packet dropping

Let P_{LD} be the threshold value of predicting Loss packets

At first, organizer node N_o has T_{MS} and N_{E_i} .

When $N_{E_{res}}$ gets less trust value than the $\frac{1}{T_{CAV_{\min}}}$ of N_{E_i} ,

Organizer node blocks the packet movement within the nodes. At that point N_i drops all the packet movement to the transfer to the misbehavior node in time T_{PM} [18].

Thus T_{PM} indicating the Time duration of predicting the misbehavior nodes and packet drop

$$T_{PM} = \left(1 - \frac{1}{T_{CAV_{\min}}}\right)\beta \tag{7}$$

And thus predicting the packet drop in the nodes by using the fuzzy based prediction model

$$P_{PD} = \frac{1}{T_{PM}}$$

$$P_{PD} = \left(\frac{T_{CAV_{\min}}}{T_{CAV_{\min}} - 1}\right) * \frac{1}{\beta} \tag{8}$$

β is energy consumption in the nodes

f. Predicting the Possibilities of Loss Packet

Sometimes, the node may accumulate with more packets because of irregular performance of the node in the server, done by few misbehavior nodes which have lesser trust value in the network server. Thus the possibility of losing packet has higher chances, in proposed methodology predicting loss packet are calculated.

$$P > P_{LP} \frac{N_{MP}}{N_{RP}} \tag{9}$$

N_{MP} denotes the movement of packet to the destination.

It's a quantity of packets received by the neighbors and N_{RP} is the packet being received by the nodes.

In case the $P > P_{LP}$, then the node is said to be malicious node and hence it has loss packet in the nodes. This methodology confirms that, there is possibility of loss packet and thus decreases the lifetime of the node. This causes the packet misfortune and however there is loss of energy in the node that leads to the loss packet.

$$E = \left(\frac{1}{N_{MP} + N_{RP}} \right) \tag{10}$$

g. Predicting Attack Precision

Precision remains for the worldwide rate of challenge. For IDS is concerned, it is difficult to maintain the attacker precision. However, in proposed method by taking the precision as a major factor to predict the attacker accuracy by means of calculating the precision for each node, yet it has been chosen as an established measure.

$$\text{Precision}_i = \frac{TN_{p_i}}{TN_{p_i} + FN_{p_i}} \tag{11}$$

Where 'I' denote the current nodes in server, TN_{p_i} is the true positive node in the system and FN_{p_i} is the false positive node in the system.

Predicting Attacker Precision is calculated by

$$P_{AP} = \frac{\sum_{i=2}^{n} TN_{pi}}{\sum_{i=2}^{n} TN_{pi} + FN_{ni}} \tag{12}$$

FN_{ni} Indicates the false negative node in the server

h. Predicting end to end delivery ratio

It is the degree of the number of packet forwarded with the trust value to the destination node and effectively all the packets are received with same trust value to the destination node in the system. Hence the acknowledgement is exchanged between the sender and receiver node in the server.

IV. PERFORMANCE EVALUATION

In hybrid & secure authentication, every member is characterized in a module independently, called fundamental rule, which elaborates about its initial state and its state transitions. We characterize two fundamental parts, as indicated in Table 1: Network Trust Administration server (NTAS) and an Organizer (N_o).

Tabulation –I

Definition of fundamental rule

Fundamental rule	**Fundamental rule configuration**
NTAS	Rule NTAS(N_o,NTNS: agent, Ka, Kr: open key, data information, Rcv: channel(dy))
N_o	Rule N_o (N_o,NTNS: agent, Ka, Kr: open key, data information, Rcv: channel(dy))

Tabulation – II

For the establishment purpose, by characterize three different conditions. Initially start with single session with all the parts played by genuine agents and prediction of attacker P_A (condition 1). After that point, next test the intruder would pose Network Trust Administration server (NTAS) (condition 2) or Organizer (N_o) (condition 2). Table 2 figure out the Hybrid& secure authentication definition of the sessions connected with each of the specified conditions, where k_x belongs to the open key of x.

Conditions	**Session Configuration**
Condition1	Session(NTAS, P_A, K_{NTMS} , K_{P_A})
Condition2	Session(NTAS, N_o , K_{NTMS} , K_{N_o})
Condition3	Session(N_o , P_A, K_{N_o} , K_{P_A})

Tabulation III

Computational Over head of Key management organization

Type of Operation	**Equation (2) Calculation Times**	**Equation (4) Calculation Times**
Symmetric Key Encryption	1	1
Symmetric Key Decryption	0	1
Asymmetric Key Encryption	1	2
Asymmetric Key Decryption	2	1
MAC	0	1

As per the above security objectives, by utilize AVISPA (Automated Validation of Internet Security Protocols and Applications) [16] system correspondence authentication security assessment framework to test the security of hybrid authentication protocol. AVISPA is a set of validation and examines the tools of security protocol [16]. It combines the two types of examinations at back ends: On-the-fly Model-Checker (OFMC), CL based Assault Searcher (CL-AtSe). The analyses are led in view of the previously stated model. For verification, utilized OFMC and CL-AtSe backend tools to predict the attacker on the authentication protocol. The test outcomes of the analysis results are summarized in Table 4. The left side list the outcome from the OFMC backend and the right section from the CL-AtSe backend tool.

Tabulation IV

OFMC [Backend]	**CL-AtSe [Backend]**
Summary	Summary
Safe	Safe
Bounded –Number of Session	Bounded –Number of Session
Protocol Secure& Hybrid Authentication	Protocol Secure& Hybrid Authentication
Statistics	Statistics
Parse Time:0.00s	Examined: 4 states
Search Time:0.02s	Reachable: 4 states
Visited Nodes:4 nodes	Translation:0.02s
Depth:2 piles	Computation:0.00s

In Hybrid Authentication Protocol, each organizer has to store two keys everlastingly: the open key SK and the NTAS's open key $NTAS_{openkey}$. Furthermore, each organizer node wants to store two nonce values: $nonce_{NTAS}$ and $nonce_{NTAS-SI}$ .Thus the organizer node attempt to access a given node, totally on authentication random basis. Average mean rate of 1/T and the next step is authentication verification from Eq.(3) in NTAS that can be modeled as a Poisson distribution with the mean 1/T.

For every validation message obtained, NTAS stores a $nonce_{NTAS}$, until it obtains the fourth step of the process of authentication message in Eq. (3) from NTAS or until a clock set to T Lifetime lapses. Assume that the T Lifetime has an upper bound and it is obtained. Whenever packet is lost, it consider a probability of packet loss in the network, the average the number of $nonce_{NTAS}$ that the Organizer must store is given by Eq. (5), where TCA signifies the average duration between the reception of an Eq. (2) message and its relating Eq.

(4) authentication message. Considering the storage overhead of $nonce_{NTAS-SI}$ and $nonce_{NTAS-SI}$ is the same. Consequently, the organizer storage over head is given in the result.

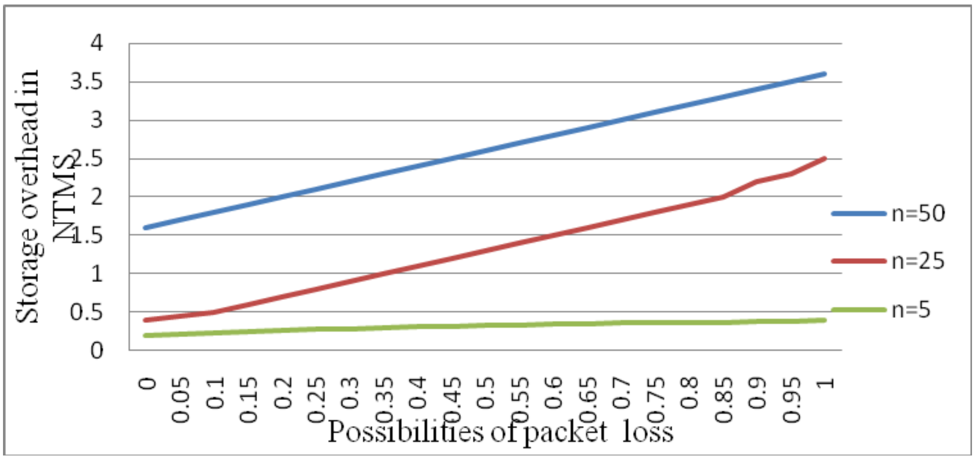


Figure 2: Storage overhead in NTAS

In Secure &Hybrid validation Protocol creates additional moves to assure the security of the system and its devices. This portion assesses the overhead of executing Hybrid authentication protocol in the Network Trust Administration Server, by considering authentication capacity and authorization capacity. Thus, it assures the credibility of the system is strong by taking both capacity and processing functionality.

V. CONCLUSION

In this research work, the proposed Secure and Hybrid authentication Protocol methodology is based on the Network Trust Administration Server & Fuzzy decision Model in order to improve the accuracy of the misbehavior nodes and detect the attacker, as well as to enhance the network security. This approach deals with the development of the network protocol, which is more suitable for Network Trust Administration Server. In this methodology, the proposed authentication protocol doesn't contain unwanted data or information, trusted authority certification on key management has high security encryption in the authentication process. Hence, this authentication protocol has more secure, highly reliable and by incorporating Fuzzy based decision model to predict the misbehavior nodes with the following parameters are considered to evaluate the performance of the proposed system such as predicting the attacker precision, prediction of packet loss and computation of storage overhead. Thus the protocols have been examined under the strongest attack model and it undergoes the nine step process which concludes that the network security is obtained in the attack model. Finally, the performance parameters are employed for determining the prediction of misbehavior nodes and its accuracy, as well as authentication protocol of proposed system under different perspectives.

VI. REFERENCES

[1] Abadeh, M. S., Habibi, J., & Lucas, C. (2007). Intrusion detection using a fuzzy genetics-based learning algorithm. Journal of Network and Computer Applications, 30(1), 414–428.

[2] Abadeh, M. S., Mohamadi, H., & Habibi, J. (2011). Design and analysis of genetic fuzzy systems for intrusion detection in computer networks. Expert Systems with Applications, 38(6), 7067–7075.

[3] Alcala-Fdez, J., Alcala, R., & Herrera, F. (2011).A fuzzy association rule-based classification model for high-dimensional problems with genetic rule selection and lateral tuning. IEEE Transactions on Fuzzy Systems, 19(5), 857–872.

[4] A. Ioannis Moschakis, H.D. Karatza. (2012). Evaluation of gang scheduling performance and cost in a cloud computing system, J. Supercomputer. 59 (2) 975–992.

[5] A. Luo, C. Lin, Z. Chen, X. Peng, et al. (2007). TNC-compatible NAC system implemented on network processor, in: The 32nd IEEE Conference on Local Computer Networks, Dublin, Ireland, pp. 1069–1075.

[6] Benferhat, S., Boudjelida, A., Tabia, K., & Drias, H. (2013). An intrusion detection and alert correlation approach based on revising probabilistic classifiers using expert knowledge. Applied Intelligence, 38(4), 520–540.

[7] Casillas, J., Cordon, O., Del Jesus, M. J., & Herrera, F. (2005). Genetic tuning of fuzzy rule deep structures preserving interpretability and its interaction with fuzzy rule set reduction. IEEE Transactions on Fuzzy Systems, 13(1), 13–29.

[8] C. Latze, U. Ultes-Nitsche, F. Baumgartner. (2007). Strong mutual authentication in a user-friendly way in EAP-TLS: software, telecommunications and computer networks, in: 15th International Conference on SoftCOM, Dubrovnik, Croatia, pp. 27–29.

[9] C. Latze, U. Ultes-Nitsche. (2008). A proof-of-concept implementation of EAP-TLS with TPM support, in: Proceedings of International Conference on Citeseer, pp. 1–12.

[10] I. Bente, J. Vieweg, J. von Helden. (2009). Privacy Enhanced Trusted Network Connect INTRUST, LNCS 6163, 2010, pp. 129–145.

[11] J. Tang, S. Song, L. Zhao, et al. (2011). Trusted network model based on trusted platform module, Computer. Eng. 37 (11) 117–119.

[12] Y. Liu, F. Zhu, Q. Shi. (2005). An improved scheme of challenge handshake authentication protocol, Computer. Eng. 31 (5) 168–169.

[13] Y. Wang, J. Wang, M. Wang, et al. (2010). Security analysis of routing protocol for MANET based on BAN logic, J. China Inst. Communication. 25 (4) 125–129.

[14] F. Dadeau, P.C. Heam, R. Kheddam. (2011). Mutation-based test generation from security protocols in HLPSL, verification and validation (ICST), in: 2011 IEEE Fourth International Conference on Software Testing, pp. 240–248.

[15] Florez, G., Bridges, S., & Vaughn, R. (2002).An improved algorithm for fuzzy data mining for intrusion detection. In Proceedings of the 21st North American Fuzzy Information Processing Society Conference (NAFIPS'02), (pp. 457–462). New Orleans, LA.

[16] Furnkranz, J. (2002). Round robin classification. Journal of Machine Learning Research, 2, 721–747.

[17] Gacto, M., Alcala, R., & Herrera, F. (2011). Interpretability of linguistic fuzzy rule based systems: An overview of interpretability measures. Information Sciences, 181(20), 4340–4360.

[18] Gomez, J. % Dasgupta, D. (2001). Evolving fuzzy classifiers for intrusion detection. In Proceedings of IEEE Workshop on Information Assurance. (pp. 68–75). United States Military Academy, West Point, New York.

[19] Kawabata Hideaki, Sueda Yoshiko, Mizuno Osamu, Nishikawa Hiroaki, Ishii Hiroshi. (2008).Self-organized key management based on trust relationship list. In: International conference on intelligence in next generation networks (ICIN).

[20] Ayed Hella, Kaffel-Ben, Belkhiri A. (2011). Toward a peer-to-peer PKI for mobile ad-hoc networks. Cyber J: Multidisc J Sci Technol, JSelect Areas Telecommunication (JSAT).

[21] Capkun Srdjan, Buttya Levente, Hubaux Jean-Pierre. (2003).Self organized public-key management for mobile ad hoc networks. IEEE Trans Mob Computer;2(1).

[22] Chan Aldar C-F. (2009). Distributed symmetric key management for mobile ad hoc networks. J Inform Process Letter;109(14).

[23] Omar Mawloud, Challal Yacine, Bouabdallah Abdelmadjid. (2009). Fully distributed trust model based on trust graph for mobile ad hoc networks. Comp Sec:199–214.

[24] Kitada Y, Takemori K, Watanabe A, Sasase I. (2005). On demand distributed public key management without considering routing tables for wireless ad hoc networks. In: 6th Asia–Pacific symposium on information and telecommunication technologies; 2005. p. 375–80.

[25] Sen Jaydip. (2010).A robust and efficient node authentication protocol for mobile ad hoc networks. In: Second international conference on computational intelligence, modeling and simulation (CIMSiM); 476–81.

[26] Djahel Soufine, Nait-Abdesselam Farid, Khokhar Ashfaq. (2008). An acknowledgment-based scheme to defend against cooperative black hole attacks in optimized link state routing protocol. In: Proc. of the IEEE international conference on communications (ICCs), p. 2780–5.

[27] Lu Songbai, Li Longxuan. (2009). SAODV: a MANET routing protocol that can withstand black hole attack. In: International conference on computational intelligence and security, IEEE Computer Society; p. 421–5.