International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 7 (2015) pp. 17933-17950

http://www.ripublication.com

Improving The Accuracy of Intrusion Detection Systems In Mobile Adhoc Network Using Fuzzy Logic Method

[1]S.Russia, [2]Dr.R.Anita, [3]K.Murugan
[1]Assistant Professor/CSE
K.S.R. Institute for Engineering and Technology
Thiruchengode
Email: russiamurugan@gmail.com
[2]Professor and Head/Dept of EEE
Institute of Road and Transport Technology
Erode 638316
[3]Assistant Professor/EEE
Institute of Road and Transport Technology
Erode 638316

Abstract

Mobile ad hoc networking (MANET) has become an agitating and significant technology in recent years because of the speedy proliferation of wireless devices. MANETs are extremely tender to aggresses attributable the open medium, dynamically interchanging network topology, combined algorithms, deficiency of centralized monitoring and management point, and lack of a absolved line of defensive structure. Due to the progression in wireless technologies, a lot of Modern epitomes have opened up for communicating. Amongst this technologies, mobile ad hoc networks act as a spectacular role for offering communication in a lot arenas because of its freelance nature of predefined infrastructure. But in terms of security system, these networks are tenderer than the ceremonious networks because firewall and gateway stationed protection mechanists can't be enforced on it. We have applied deposited width clustering algorithmic program for effective signal detection of the anomalies in the MANET traffic and likewise engendered a different cases of attacks in the network. Intrusion Detection System (IDS) may accumulate and examine audit data point for the whole network. This paper accentuated upon proposed fuzzy based intrusion detection systems in MANET and awarded their effectivity to distinguish the intrusions. This paper also analyzes the disadvantages of fuzzy based intrusion detection systems and discoursed the future guidance in the area of intrusion detection for mobile ad hoc networks.

Key words— Mobile Ad Hoc Networks (MANETs), Detection Methods, Fuzzy Logic, Intrusion detection system (IDS), Cross layer, Security issues.

Introduction

In recent classes, with the speedy proliferation of wireless devices, for example., mobile laptop computers, PDAs, and wireless telephones, the potentialities and grandness of mobile ad hoc networking have become manifest. A mobile ad hoc network (MANET) is conceived along a radical of mobile wireless nodes frequently without the help of fixed network infrastructure. The nodes must collaborate through forwarding packets so that nodes on the far side radio communication ranges can intercommunicate with each other. There are a number of significant MANET application program*, for example., battlefield functioning, emergency rescues, mobile conferencing, rest home and biotic community networking, and sensor dust [1].

An intrusion is specified as any set of activeness that endeavour to compromise the unity, confidentiality or accessibility of a resource. Intrusion detection is separated into two eccentrics: misuse intrusion detection and anomaly intrusion detection. Misuse intrusion detection roles well-defined approach pattern* of the aggress that exploit weaknesses in scheme and application software system to distinguish the intrusions. These radiation pattern* are enciphered in advance and utilized to play off versus the user behavior to observe intrusion. Anomaly intrusion detection applies the average use of demeanour patterns to distinguish the intrusion. The regular usage patterns are fabricated from the statistical measurements of the system characteristics. The demeanour of the user is noticed and whatever difference from the fabricated regular demeanour is observed as an intrusion. In Distributed Intrusion Detection System (DIDS) conventional intrusion detection system are embedded interior reasoning factors and are deployed across a huge network. In a distributed surroundings, IDS factors intercommunicate with each other, or with a fundamental host. Along bearing these conjunctive factors disseminated across a network, incidental analysts, network functioning, and security personnel department are capable to get a more encompassing aspect of what is happening on their network as a whole thing. Distributed monitoring allows for early detecting of contrived and interconnected assaults, there by admitting network administrators to take encumbrance measurements. DIDS also assists to control the dispersing of worms, ameliorates network monitoring and incidental analysis, attack hounding and so on. It also assists to observe new-fangled threats from unauthorised exploiters, back-door aggressors and hackers to the network across multiple emplacements, which are geographically differentiated.

MANETs are much more tender to aggresses than wired (conventional) networks due to the open mass medium, dynamically commuting network topology, combined algorithmic program, lack of concentrated monitoring and management point, and deficiency of a clear line of defence. There are modern research campaigns, in assuring the ad hoc routing communications protocol. Most of these are prevention methods. Experience in security research in the cabled surrounds has instructed us that we require to deploy defence-in-depth or superimposed security mechanises because security is a mainframe a chain) that is as ensure as its most weakness link [2]. Besides

prevention, we also require detection and reaction, as well as security policies and exposure analysis. While a lot of intrusion detection (ID) methods have been highly-developed in the wired networks, the immense differences in MANET need that we figure Modern intrusion detection architectures and algorithmic program.

In this paper, we reputation our advance in acquiring ID potentialities for MANET. We firstly afford an overview of the primary approximations and final result.

It is hard for Intrusion Detection system (IDS) to fully observe routing aggresses due to MANET's device characteristic. And so, the IDS requires an ascendable architecture to accumulate adequate manifests to detect those aggresses efficaciously. A malicious node might accept advantages of the MANET node to establish routing aggresses as the node plays router to intercommunicate on one another. The wireless links among the nodes along with the mobility advances the disputes of IDS to notice aggresses. Therefore, we are prompted to intent a fresh IDS architecture which affects cross layer design to expeditiously detect the abnormal condition in the wireless networks. We have proposed afresh intrusion detection architecture which integrates cross layer that interacts among the layers. In addition to these we have expended connection module to link amongst the OSI protocol stack and the IDS module which resultants in low overhead on the data point accumulation. We have applied the fixed width clustering algorithm in anomalousness detection locomotive for effective detection of intrusion in the ad hoc networks.

Literature Survey

Several analyses have been finished on security prevention evaluates for infrastructure-based wireless networks but fewer processes has been done on the expectation of intrusion detection. A few universal approach has been utilized in a circularized mode to ensure the legitimacy and unity of routing data such as key generation and management on the prevention face. Authentication stationed approaches are utilized to protected the unity and the authenticity of routing substances such as [2], [3]. There are few troubles that have to be confronted in recognizing a few of the systems like cryptology and they are comparatively unaffordable on MANET because of computational capacitance. A number of intrusion detection schemes for intrusion detection system have been acquainted for ad-hoc networks. In [4], the paper purposed architecture for a distributed and combined intrusion detection system for ad-hoc networks established on statistical anomalousness detection processes but they have not the right way to adverted about the simulation scenario and the type of mobility they have utilized. In [5], A. Mishra accents the dispute for encroachment detection in ad-hoc network and determination the use of anomalousness detection, but do not allow a elaborated result or implementation for the problem. In [6], Huang points an anomalousness detection method that researches the coefficients of correlation among the features of nodes and discourses about the routing anomalousnesses. In [7] introduces an intrusion detection technique practicing a clustering algorithm for routing aggresses in sensor networks. It is capable to observe three significant characters of routing attacks. They are capable to observe sink hole attacks efficaciously which are intense frame of attack. There are a few defects alike there is

absence of simulation program that can accompaniment a broader assortment of aggresses on bigger scale networks. Fixed width clustering algorithm has displayed to be extremely efficient for anomalousness detecting in network intrusion. It introduces a geometrical model for unsupervised anomalousness detection. This paper requires more characteristic mappings across a different forms of data point and requires to execute more extended experimentations evaluating the techniques represented.

Furthermore, a number of confidence making and cluster-based voting systems have been proposed to enable the share-out and vetting of messages, and information, rendered and accumulated by IDS schemes. Zhang and Lee distinguish a distributive and cooperative anomalousness detection-based IDS for ad hoc networks [2, 3]. Tseng et al. Identify an approach that implies the use of impermanent state machines for assigning right AODV routing demeanour and distributed network monitors for observing run-time violation of the stipulations [8]. Pirzada and McDonald introduce a technique for building assurance evaluates of route trustiness without a fundamental trust agency. The authors also introduce a compact summary of premature work in the area of constituting trust in ad hoc networks [5]. Theodorakopoulos and Baras introduce a technique for building trust metric function and evaluating trust [6]. Michiardi and Molva allot a value to the “reputation” of a node and use this selective information to distinguish misbehaving nodes and collaborate alone with nodes with trusted reputations [7]. Albers and Camp couple a trust-based mechanics with a mobile factor established intrusion detection scheme, but do not hash out the security significances or elevated required to ensure the network and separate nodes from the mobile factors themselves [8]. Sun, Wu and Pooch present a geographical zone-based intrusion detection framing that applies location-aware partition gateway nodes to accumulate and combine alarms from intra partition nodes. Gateway nodes in adjacent zones could so additional collaborate to execute intrusion detection projects in a broader area and try to concentrate false positive alarms [9].

Intrusion Detection System

When some set of activities endeavour to compromise with the security system imputes specified confidentiality, repudiation, availableness and integrity of resources then these accomplishes are said to be the intrusions and spotting of such intrusions is called intrusion detection system (IDS) [10]. The most common functionality of IDS reckons alone upon three important modules such as data accumulation, detection and response modules. The data accumulation module is responsible for accumulating data from several data sources such as system audit information, network traffic data point, etc. Detection module is responsible for analysis of accumulated information.

Although detecting intrusions if detecting module observes some mistrustful action in the network then it inducts reaction by the response module. There are three primary detection methods introduced in the literature such as pervert based, anomalousness based and stipulation based methods. The beginning process, pervert based detection systems such as IDIOT and STAT detect the intrusions on the behalf of predefined aggress key signature. The disfavour of these method is that it can't detect modern attacks but has low false positive rate so that it is usually utilized by the technical

design based IDSs. Second intrusion detection method is anomalousness placed detection method e.g. IDES [11]. It detects the intrusion on establishes of convention demeanour of the system. Defining the standard demeanour of the arrangement is a very ambitious task since demeanour of arrangement can be altered time to time. This method could notice the Modern or unknown aggresses but with eminent false positive rates. The third method is stipulation - based intrusion detection.

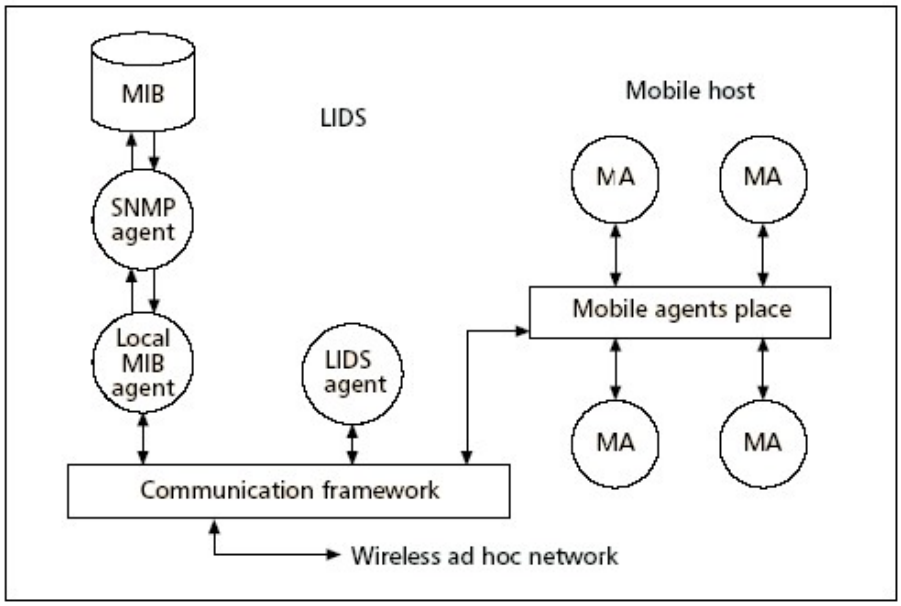


Figure 1: Local Intrusion Detection System (LIDS) Architecture

In this detection technique, foremost assigned the set of restraints on a peculiar protocol or program and so notice the intrusions at run time encroachment of these stipulations. The independent trouble with this method that it chooses a lot of time for specifying the stipulation that's why it is a time consuming method [12]. About the grounds of the audited account data point, Intrusion detection system can be server based and network based. Server based IDS accumulate the audit data point from operating system at a specific server and network based intrusion detection system accumulates audited account data point from server as comfortably as tracing the network traffic for any type of untrusting activeness. Usually there are three most common cases of IDS architecture in literature: Stand-alone intrusion detection systems - In this type of intrusion detection system architecture, an IDS execute severally on each node in the network; Distributed and Cooperative intrusion detection systems - In this architecture whole nodes have IDS factors so that each node can participate in intrusion detection locally and depend upon amenability among the nodes it can be made conclusion globally. This architecture dependant IDS are capable to attain two cases of decision that is collaborative and independent. In collaborative decision, altogether nodes participate actively to construct decision just in case of independent decision a few specific nodes are responsible for building decision. Hierarchical Intrusion Detection Systems. For each one cluster has cluster head which

has a lot of irresponsible than the another node members in the clustering [10] [11]. We will talk about fuzzy logical system based proposed IDSs for MANETs in additional segments.

Methodology

Fuzzy Rule-Based Systems

Fuzzy logic has proved to be a powerful tool for decision making to handle and manipulate imprecise and noisy data. The notion central to fuzzy systems is that truth values (in fuzzy logic) or membership values (in fuzzy sets) are indicated by a value in the range [0.0, 1.0], with 0.0 representing absolute falseness and 1.0 representing absolute truth. A fuzzy system is characterized by a set of linguistic statements based on expert knowledge. The expert knowledge is usually in the form of if-then rules.

Definition 1:.Let X be some set of objects, with elements noted as x. Thus, $X = \{x\}$

Definition 2:.A fuzzy set A in X is characterized by a membership function which are easily implemented by fuzzy conditional statements. In the case of fuzzy statement if the antecedent is true to some degree of membership then the consequent is also true to that same degree.

A simple rule structure: If antecedent then consequent.

A simple rule: If variable$_1$ is low and variable$_2$ is high then output is benign else output is malignant.

In a fuzzy classification system, a case or an object can be classified by applying a set of fuzzy rules based on the linguistic values of its attributes. Every rule has a weight, which is a number between 0 and 1 and this is applied to the number given by the antecedent. It involves 2 distinct parts. First the antecedent is evaluated, which involves fuzzifying the input and applying any necessary fuzzy operators and second applying that result to the consequent known as inference. To build a fuzzy classification system, the most difficult task is to find a set of fuzzy rules pertaining to the specific classification problem. We explored three fuzzy rule generation methods for intrusion detection systems. Let us assume that we have an-dimensional *c*-class pattern classification problem whose pattern space is an *n*-dimensional unit cube [0, 1]^n. We also assume that m patterns $xp = (x_{pl}, ..., x_{pn})$, p=1,2,…,m, are given for generating fuzzy if-then rules where $x_p \in [0,1]$ for p=1,2,…,m.

Each attribute is partitioned into 20 membership functions $f_h(.) h = 1, 2, ..., 20.$ The smoothed histogram $m_i^k(x_i)$ of class k patterns for the ith attribute is calculated using the 20 membership functions $f_h(.)$ as follows:

$$m_i^k(x_i) = \frac{1}{m^k} \sum_{xp \in class\ k} f_h(x_{pi}) \qquad (1)$$

$$for\ \beta_{h-1} \le x_i \le \beta_h,\ h = 1, 2, ..., 20,$$

Where m_k is the number of class k patterns, $[\beta_{h-1}, \beta_h]$ is the h^{th} crisp interval corresponding to the 0.5-level set of the membership function $f_h(.)$

$$\beta_1 = 0, \beta_{20} = 1, \tag{2}$$

$$\beta_h = \frac{1}{20-1}\left(h - \frac{1}{2}\right) for\ h = 1, 2, ..., 19. \tag{3}$$

The smoothed histogram in (1) is normalized so that its maximum value is 1. A single fuzzy if-then rule is generated for each class. The fuzzy if-then rule for the kth class can be written as

if x_1 is A_1^k and... and x_n then class k,

Where A_1^k is an antecedent fuzzy set for the ith attribute. The membership function of A_1^k is specified as

$$A_1^k(x_i) = \exp\left(-\frac{(xi - \mu_i^k)^2}{2(\sigma_i^k)^2}\right), \tag{4}$$

Where μ_i^k is the mean of the ith attribute values x_{pi} of class k patterns, and σ_i^k is the standard deviation. Fuzzy if-then rules for the two-dimensional two-class pattern classification problem are written as follows:

If x_3 is A_3^1 and x_4 is A_4^1 then class 2,

If x_3 is A_3^2 and x_4 is A_4^2 then class 3,

Membership function of each antecedent fuzzy set is specified by the mean and the standard deviation of attribute values. For a new pattern $x_p = (x_{p3}, x_{p4})$ the winner rule is determined as follows:

$$A_3^*(x_{p3}).A_2^*(x_{p4}) = \max\left\{A_1^k(x_{p3}).A_2^k(x_{p4}) \mid k = 1, 2\right\}. \tag{5}$$

Step 1: Calculate the compatibility of each training pattern $(x_p = x_{p1}, x_{p2}, ..., x_{pn})$ with the *j*th fuzzy if-then rule by the following product operation:

$$\pi_j(x_p) = A_{j1}(x_{p1}) \times .... \times A_{jn}(x_{pn}),\ p = 1, 2, ..., m. \tag{6}$$

Step 2: For each class, calculate the sum of the compatibility grades of the training patterns with the *j*th fuzzy if-then rule R_j.

$$\beta_{class\ k_j^*}(R_j) = \sum_{xp\ class\ k}^{n} \pi(x_p), K = 1, 2, ..., c, \tag{7}$$

Where $\beta_{class\ k_j^*}(R_j)$ the sum of the compatibility grades of the training patterns in class k with the *j*th fuzzy if-then rule (R_j).

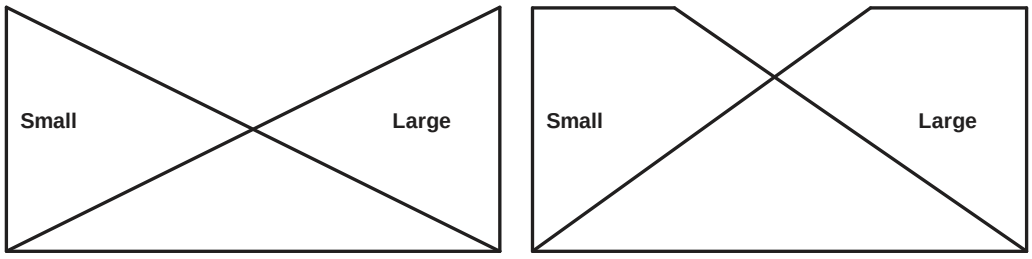
Step 3: Find class A_j^* that has the maximum value $\beta_{class\ k_j^*}(R_j)$.

$$\beta_{class\ k_j^*} = Max\left\{\beta_{class\ 1}(R_j),...,\beta_{class\ c}(R_j)\right\}. \quad (8)$$

If two or more classes take the maximum value or no training pattern compatible with the *j*th fuzzy if-then rule the consequent class C_i cannot be determined uniquely. In this case, let C_i be

Step 4: If the consequent class C_i is 0, let the grade of certainty CF_j be $CF_j = 0$. Otherwise the grade of certainty CF_j is determined as follows:

$$CF_j = \frac{(\beta_{class\ k_j^*}(R_j) - \overline{\beta}}{\sum_{k=1}^{c} \beta_{class\ k}(R_j)}, \quad (9)$$



(a) (b)

Figure 2: Fuzzy partition of each attribute: (a) simple fuzzy grid approach; (b) modified fuzzy grid approach.

where

$$\overline{\beta} = \sum_{\substack{k=1 \\ k \neq k_j^*}} \frac{\beta_{class\ k}(R_j)}{(c-1)}, \quad (10)$$

The above approach could be modified by partitioning only the overlapping areas as illustrated in Fig. 3.

This approach generates fuzzy if-then rules in the same manner as the simple fuzzy grid approach except for the specification of each membership function. Because this approach utilizes the information about training patterns for specifying each membership function as mentioned in Section 3.1, the performance of generated fuzzy if-then rules is good even when we do not use the certainty grade of each rule in the classification phase. In this approach, the effect of introducing the certainty grade to each rule is not so important when compared to conventional grid partitioning.

Neural Learning of Fuzzy Rules (FR_3)

In a fused neuro-fuzzy architecture, neural network learning algorithms are used to determine the parameters of fuzzy inference system (membership functions and number of rules). An Evolving Fuzzy Neural Network implements a Mamdani-type

FIS and all nodes are created during learning. Each input variable is represented here by a group of spatially arranged neurons to represent a fuzzy quantization of this variable. New neurons can evolve in this layer if, for a given input vector, the corresponding variable value does not belong to any of the existing MF to a degree greater than a membership threshold.

Proposed Method

The detection technique is based on analyzing the incoming traffic from neighboring nodes on a hop along the path to the BS. During the initialization phase, when it is assumed that no attacker to be active in the area of WSN, nodes gather data from their neighbors jumped and create profiles of their normal behaviors. During the course of the operating time of the network traffic anomalies are identified by comparison of newly acquired data to normal profiles. Then the fuzzy inference system the final conclusion on the basis of the preliminary analysis is derived and decides whether an attack is. Actually, a behavioral profile comprises a neighboring thresholds for the chosen parameters of the traffic that is produced by this node. Since the method is based on the statistical estimate of the probability distributions of the monitored attributes, is efficient and reliable. Since thresholding technique is based on simple statistical methods and does not require large samples for estimation of parameters, threshold values can be easily upgraded in changing environmental conditions or application. The contributions to research in each field are summarized and compared, allowing us to clearly define the existing research challenges and highlight promising new research directions systematically. The results of this review should provide useful information about the current literature IDS and be a good source for anyone interested in implementing CI is about the IDS or related fields.

We have utilized some techniques in Intrusion detection module ready to amend the efficiency and strength of the MANET nodes. On our analyzes, we have discovered that among all the data mining intrusion detection techniques, clustering-based intrusion detection is the most possible one because of its power to detect new attacks. A lot of traditional intrusion detection methods are limited with accumulation of training data from real networks and manually labeled as normal or abnormal. It is very time consuming and expensive to manually accumulate pure normal data and separate data in wireless networks.

Latest research findings on IDPSs are organized in terms of layered taxonomy and discussed in two parts. The first part provides an insight view on recent proposed systems in terms of their structure, technology, processes of audit data collection and analysis, detection techniques, and types of responses. The second part only targets the research studies on alarm management which have focused on false positive alarm reduction by applying various methods for different IDPS detection techniques.

Their proposed technique supported high detection accuracy with least false alarms, but trades-off a lack of program semantics for greater malware resistance and ease of deployment [12]. We have applied association algorithm such as Apriori which can be used to accomplish traffic features which is then accompanied by clustering algorithm. In [14], it states that a beneficial efficiency and execution is received with association

algorithm and clustering algorithm. The association rule and clustering are used as the root for attendant anomaly detection of routing and other attacks in MANET. Our proposed IDS architecture is shown in fig. 4 and the IDS module is described below [15].

Local Detection

The local detection module consists of anomaly detection engine. The local detection module analyzes the traces of local data collected by the collection module local data for evidence of anomalies. A normal profile is an aggregate set of multiple training data segments rule. New and updated detection rules through ad-hoc networks are obtained from normal profile. The normal profile is normal behavior patterns calculated using data from monitoring a training process in all activities are normal. During testing, normal and abnormal activities are processed and deviations from normal profiles are recorded. Anomaly detection distinguishes normal and abnormal deviation data by comparing the profiles of test data with predicted normal profiles. If the detection rules deviate beyond a threshold range and if you have a very high accuracy rate can be determined independently that the network is under attack and alert management starts.

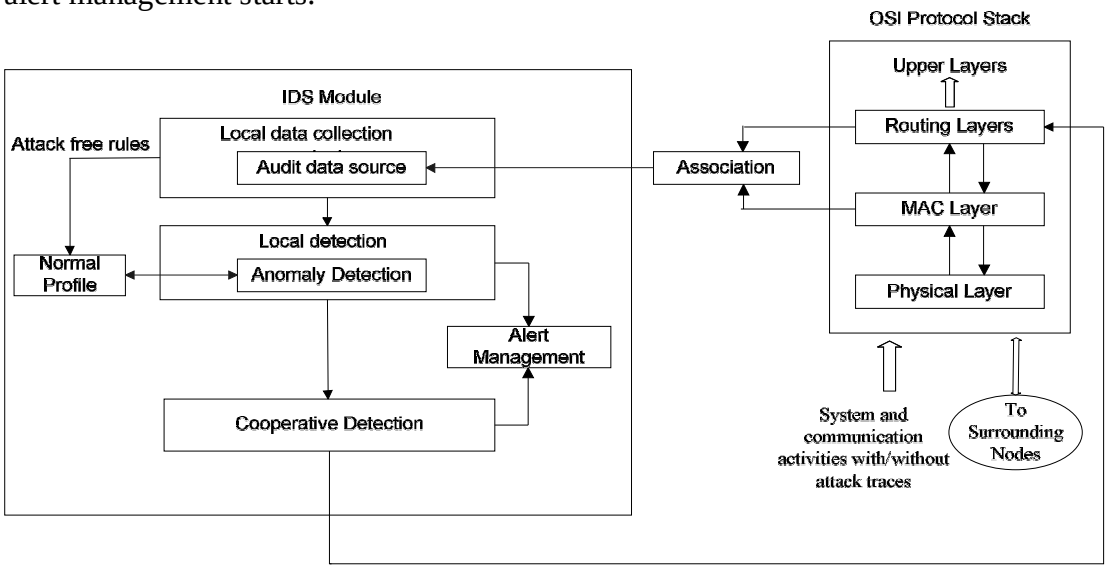


Figure 3: Proposed IDS Architecture in MANET

Cooperative Detection

When the level of support and confidence is low or penetration testing is weak and inconclusive in the detection node then you can decide for collaboration by collecting information through the points surrounding through communication channel protected. The decision of the cooperative detection is based on the majority vote of the reports received indicate an intrusion or anomaly.

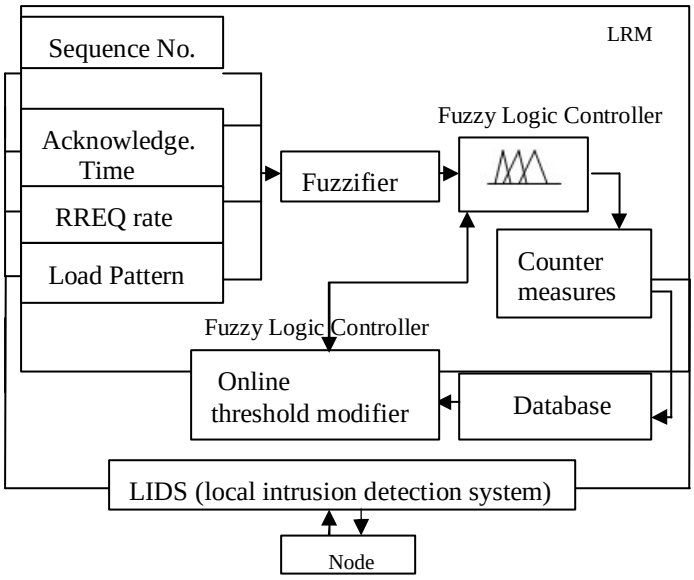


Figure 4: Proposed Fuzzy Controller Based IDS

The rule for detecting a fuzzy model based attack and for the development of the function were formed membership, the input parameters such as the ratio of forward packet and the average number of selected target sequence in each time slot. The output of the rule depends on the level derived fidelity of each node whose value is between 0 to 10 and the threshold level chosen fidelity 5.5 to analyze the node level. If the calculated level of fidelity node is less than or equal to the threshold value of fidelity to blackhole node is then otherwise is not blackhole node. Ultimately level of fidelity shows the node level.

This scheme is useful for detecting black hole attack, but cannot detect new attack. In literature, there are other approaches also available for the black hole attack detection using fuzzy logic a direct based IDS diffuse appears that packages can detect attack falling hole as hole Black and gray attack. They considered that each node is having IDS and malicious activity at the local level for this purpose and a threshold value for each node is assumed. In this proposed approach, each node maintains its list of packages using the tool: Sequence no, source node, destination node, packet type and expiration time. During the analysis, some indications on the basis of degree of symptoms are calculated, the frequency of occurrence of symptoms and confirmed the presence of attack. On the basis of analysis result, it was shown that fuzzy logic is able to find more accurately proposed attack. This scheme chosen threshold value for each node is very confusing work.

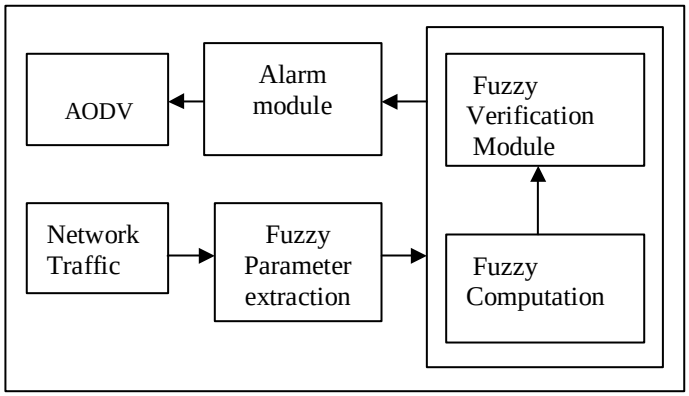


Figure 5: Fuzzy based IDS

Experimental Results

The nodes intercommunicate applying 10 constant bit rate (CBR) node-to-node connectors with a data point rate of 4 packages per sec. Entire nodes pull in stochastic manner with accelerate varied from 0 m/s to 3 m/s. The computer simulation clip is 100 secs. Altogether experimentations, misdemeanant nodes are nodes that correspond to forward packages (they don't vary the contented of packages) and then betray to do due to overburden, selfishness, spitefulness, or brokenness. In our simulations, the misconducting nodes can impairment the network functioning particularly by incorrectly describing that other pattern nodes as misbehaving. We set up specialised tending on however these malicious accomplish impact network execution. Of the 50 nodes in the simulated network, a few variable quantity percentages of the nodes misconduct. The percentage of misconducting nodes changes from 0% to 40% in 10% growths. Firstly we execute the simulation with 30% misconducting nodes which misconduct as incorrectly describing. And then we replicate the experimentations with 80% misconducting nodes which misconduct as incorrectly describing.

Table 1: Configuration Parameters

Time interval (TI)	100 seconds
Training period (*N*)	5 TIs
Testing period	15 TIs
Number of intruders	Varying from 1 to 5
Chi-square test (α)	5% (i.e. 95% confidence interval)
Test Sliding Window (TSW)	5 TIs
Number of Parameters	PM=4 & NCM=7 parameters
Intrusion Response Actions	Complete Isolation, Route Around Attacker & No Punishment
Confidence on attack	Function of: Confidence Interval of

Network Performance Degradation	Function of: Network Throughput, PDR, RPO & RPD
COA & NPD levels	4 (Low, Medium, High & Very High)

We utilize the equivalent metric function with [18] to measure our extension: Throughput and Overhead. Throughput is the percentage of sent off data packages actually obtained by the intended addresses. Overhead is the ratio of routing linked up transmission system to data point transmission system in a simulation. We alter the percentage of typically misconducting nodes from 0% to the maximum 40%, with the percentage of incorrectly reporting misdemeanant nodes fixated at 30%.

In that scenario, we study the effectivity of the intrusion response system utilizing NPD as a system of measurement. We conceive 25 and 50 node networks, both with assorted attacks and also with compounding of a different synchronous attacks. We executed 30 runs with each aggress in a 25 node network, these representing 10 runs while IDS doesn't respond to intrusion, 10 runs when IDS responds with a fixated response (isolate interloper) altogether cases, and 10 runs while IDS hires the adaptive compromising intrusion response system. We also ingeminated this examines with a 50 node network.

The charts of Fig. 7 and 8 shows the effectivity of the intrusion response system in terms of the NPD, for 25 and 50 node networks respectively. They establish the NPD in several attack positions when there has no more response to intrusion by IDS, when the response comprises interloper isolation, and in the adaptive response encase. It can be considered from the charts that the intermediate network debasement is reduced when IDS is utilized with the adaptive compromising intrusion response system proposed in this paper. While IDS denigrates the impairment to network functioning in all attacks, we detect that in the case of modest attacks such as rushing along or a few GH attacks, the adaptive response importantly reduces the network abasement.

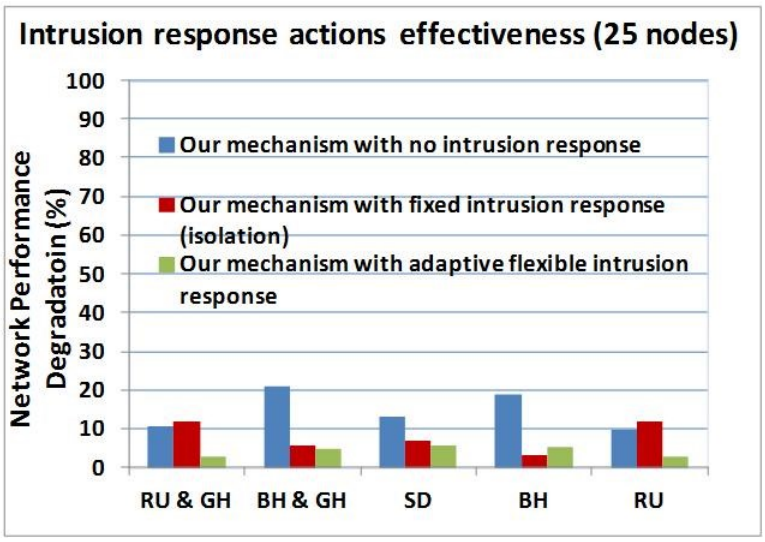


Figure 6: IRA Effectiveness With Various Attacks In 25 Node Scenario

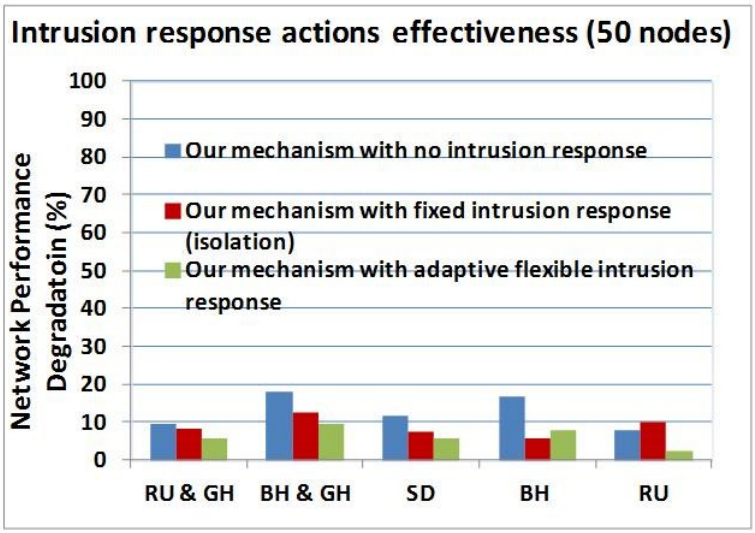


Figure 7: IRA Effectiveness With Various Attacks In 50 Node Scenario

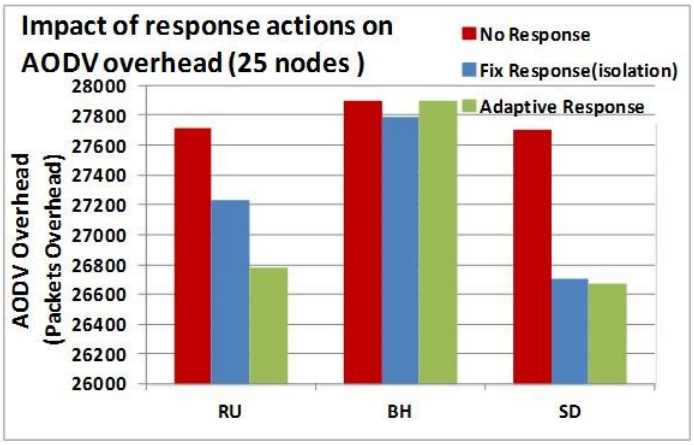


Figure 8: Impact of IRA on AODV Overhead With BH, RU And SD Attack In 25 Node Network

Table 2: Comparison of Cost Sensitive Intrusion Response Model [13] and IDS

Comparing Parameter	Cost Sensitive Model [13]	IDS
Intrusion response selection criteria	Topology Dependency Index (TDI) and Attack Damage Index (ADI)	Confidence on Attack (COA) and Network Performance Degradation (NPD)
Intrusion response actions	Normal, Recovery, Full isolation, Temporary isolation and Relocation	Isolation, Route around attacker, and No punishment
Types of attacks considered	Authenticity, Integrity and Availability	Black hole, Sleep deprivation, Rushing, Grey hole
Parameter for intrusion response impact assessment	Packet Delivery Ratio (PDR)	Network Performance Degradation (Eq.5)

Impact of intrusion response scheme	Max PDR reduction = 13 %	Maximum NPD = 7 %
Scalability	Simulated up to 50 nodes	Simulated up to 200 nodes
Network overhead	Not considered	Less than 5 % of total network traffic

Table 2 equates the monetary value sensitive intrusion response framework with IDS. The TDI corresponds the routing habituation of nodes on the interloper and the ADI corresponds the damage caused by an attacker.

Table 2: Performance Comparison Using Existing and Proposed Method

Type of attack	Classification Accuracy %	
	NN	FCM
Normal	99.56	99.57
Probe	99.88	94.62
DOS	98.99	98.97
U2R	65.00	59.00
R2L	97.26	97.02

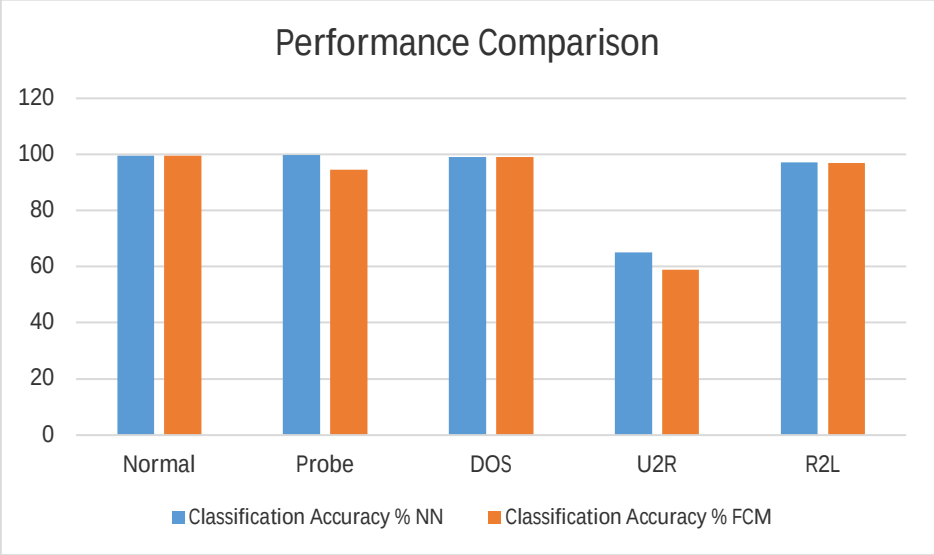


Figure 9: Performance Comparison Using Existing and Proposed Method

Neural Network (NN) uses a hybrid learning technique (a mixture of unsupervised and supervised learning) to fine-tune the parameters of the FIS. As NN adopts a single pass training (1 epoch) it is more adaptable and easy for further on-line training, which might be highly useful for online detection and updating the knowledge base. Another important feature of NN is that the user has the flexibility to construct the network (by selecting the parameters). However, IDS swears on assurance in detected

attack and it has impact during network functioning. The simulation in [19] controls using five cases of intrusion response (standard, retrieval, full isolation, impermanent isolation and transplantation). IDS reacts to the intrusion by adaptively choosing among the three reactions (isolation, route around aggressor, and no punishment). Both the cost sensible modelling [13] and IDS have been applied using GloMoSim. Generally the comparability appearances that IDS is better in terms of rising network functioning in respective attacks with minimal overhead on the network.

Conclusion

IDS can't only detect a number of aggresses but can also adaptively react to the detected attacks to block the attack and / or extenuate the impairment stimulated by the attack and preclude additional attacks from the intrusive nodes. Our intrusion response system has an attenuate effect on network functioning, and acts by adaptively choosing the intrusion response action established on the degree of confidence in the detection of the attack, the attack stiffness and the abjection in network execution. We have examined the functioning manner of proposed fuzzy based IDSs and accomplished on decision that still we don't have some anticipating resolution for this dynamical surroundings because most of Proposed fuzzy based IDSs accentuated on very limited characteristics for data point accumulation towards detection of very particular range of attacks.

Future Works

We require to assure that the IDS can't be compromised, or at least, attacks versus the IDS can be noticed. This is peculiarly significant while applying the cluster-based detection approaching. If a compromised node takes place to be elected as the cluster head, it can establish attacks without being observed because it is the single node that should run an IDS and its IDS might have been out of action already. A solution mayhap to apply a tamper-resistant device to protect the IDS on each node. We will further investigate this issue. This problem can be partially resolved by implementing certification on all packets. However, a few routing linked attacks can still be established without required to hide out or spoof because by the time an anomalousness is described, it may already be too late to correlate the abnormal behavior with packets prescriptive before.

Reference

[1] Chaudhary, A., Tiwari, V. N., & Kumar, A. (2014). Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks. Bharati Vidyapeeth’s Institute of Computer Applications and Management (BVICAM), 6(1), 690-696.

[2] Shah, N., & Valiveti, S. (2012). Intrusion detection systems for the availability attacks in ad-hoc networks. International Journal of Electronics

and Computer Science Engineering (IJECSE, ISSN: 2277-1956), 1(03), 1850-1857.

[3] Chaudhary, A., Tiwari, V., & Kumar, A. (2014, May). A novel intrusion detection system for ad hoc flooding attack using fuzzy logic in mobile ad hoc networks. In Recent Advances and Innovations in Engineering (ICRAIE), 2014 (pp. 1-4). IEEE.

[4] Bu, S., Yu, F. R., Liu, X. P., & Tang, H. (2011). Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks. Wireless Communications, IEEE Transactions on, 10(9), 3064-3073.

[5] Chaudhary, A., Tiwari, V. N., & Kumar, A. (2015). A Cooperative Intrusion Detection System for Sleep Deprivation Attack Using Neuro-Fuzzy Classifier in Mobile Ad Hoc Networks. In Computational Intelligence in Data Mining-Volume 2 (pp. 345-353). Springer India.

[6] Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion detection systems in wireless sensor networks: a review. International Journal of Distributed Sensor Networks, 2013.

[7] Krishnan, M. M., & Khader, P. S. A. (2012). Fuzzy Based Integrated Security Model for Mobile Ad Hoc Network. In Global Trends in Computing and Communication Systems (pp. 467-472). Springer Berlin Heidelberg.

[8] Bu, S., Yu, F. R., Liu, X. P., Mason, P., & Tang, H. (2011). Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. Vehicular Technology, IEEE Transactions on, 60(3), 1025-1036.

[9] Govindan, K., & Mohapatra, P. (2012). Trust computations and trust dynamics in mobile adhoc networks: a survey. Communications Surveys & Tutorials, IEEE, 14(2), 279-298.

[10] Mukhopadhyay, A., Das, S., & Sadhukhan, S. K. (2013). Vulnerable Path Determination in mobile ad-hoc networks using Markov Model.

[11] Butun, I., Morgera, S. D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. Communications Surveys & Tutorials, IEEE, 16(1), 266-282.

[12] Xia, H., Jia, Z., Li, X., Ju, L., & Sha, E. H. M. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Networks, 11(7), 2096-2114.

[13] Wahengbam, M., & Marchang, N. (2012, March). Intrusion detection in manet using fuzzy logic. In Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on (pp. 189-192). IEEE.

[14] Vydeki, D., & Bhuvaneswaran, R. S. (2013). Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks. Journal of Computer Science, 9(4), 521.

[15] Chaudhary, A., Tiwari, V. N., & Kumar, A. (2014, February). Design an anomaly based fuzzy intrusion detection system for packet dropping attack

in mobile ad hoc networks. In Advance Computing Conference (IACC), 2014 IEEE International (pp. 256-261). IEEE.

[16] Das, N., & Sarkar, T. (2014). Survey on Host and Network Based Intrusion Detection System. Int. J. Advanced Networking and Applications, 6(2), 2266-2269.

[17] Ganapathy, S., Yogesh, P., & Kannan, A. (2011). An intelligent intrusion detection system for mobile ad-hoc networks using classification techniques. In Advances in Power Electronics and Instrumentation Engineering (pp. 117-122). Springer Berlin Heidelberg.

[18] Pastrana, S., Mitrokotsa, A., Orfila, A., & Peris-Lopez, P. (2012). Evaluation of classification algorithms for intrusion detection in MANETs. Knowledge-Based Systems, 36, 217-225.

[19] Anusha, K., Jayaleshwari, N., Arun Kumar, S., & Rajyalakshmi, G. V. (2013). An Efficient And Secure Intrusion Detection Method In Mobile Adhoc Network Using Intuitionistic Fuzzy. International Journal of Engineering and Technology (IJET) Vol, 5.