A Novel Based Fuzzy Cognitive Maps Protocol for Intrusion Discovery in Manets

D.Rajalakshmi, K.Meena

Abstract: ***A MANET's affords the communication among several nodes via a shared wireless channel. Communication is done without the support of a stable network structure. Since the purpose of wireless networks has improved, safety inside the MANET's come to be further essential consequently. This situation will be active and competent for discovering intrusions. An effective intrusion discovery system properly finds the regular and mischievous node events. The numbers of new attacks are enlarged rapidly and attacks must be discovered earlier they be capable of do any maltreatment to the systems or data. Intrusion discovery system focuses to discover threats on mobile nodes or intrusions in that ad hoc network. Here, proposing a proficient system for examining also discovering a mischievous nodes using Fuzzy Cognitive Maps (FCM's) protocol. Using Fuzzy Cognitive Maps protocol in order to discover the mischievous node with great precision and less erroneousness as well as it helps to develop the performance of a system.***

Keywords: MANET, Intrusion Detection, Security, AODV and FCMs

I. INTRODUCTION

A MANET is an arrangement of the communication system, mobility nodes are can easily; energetically self-organize in random and provisional network topologies without the necessity of a wired support or a consolidated supervision [1]. Persons and the relevant strategies may be flawlessly data networked in regions, externally any preexistent transmission structure in other words while the usage of such structure needs wireless allowance. Mobile ad hoc networking offers distinctive benefits and changeability for certain atmospheres and applications. First, since they have no stable structure containing base stations as requisites, they can be formed and used anytime, everywhere. Second, such networks can be essentially fault resistant, for they do not control under the boundaries of a stable topology. Really subsequently all nodes are permitted to be mobile, the structure of such networks is automatically time changing [2]. Addition and omission of nodes ensues only by communications with other nodes; no other organization is involved.

Fig.1. shows a design of mobile ad hoc network, it involves several nodes. Every node are capable to speaks directly with alternative nodes that live among its transmission vary. For act with nodes that live on the far side this vary, the node desires to transitional nodes to convey information by hop by hop. The information is shifted from Supply to destination via node 1 and node 2.

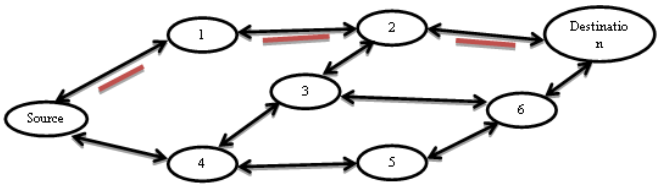

Fig.1. Mobile Ad hoc Network

MANETs receive common features found in wireless networks and precise features of ad hoc networking [3]:

- Wireless: Leaf nodes interconnect wirelessly and communicate the relevant information (radio, infrared, etc.,)
- Ad hoc based: It's a short-term network designed vigorously in a random method by a group of leaf nodes as necessity rises.
- Independent and Arrangement less: MANET doesn't be contingent on federal supervision. Each leaf node works in disseminated peer-to-peer mode, acts as an autonomous router, and produces self-governing information.
- Multi-hop routing: Every leaf node behaves as a router and sends every other's information to permit data distribution among mobile nodes.
- Mobility: Every leaf node is absolve to move concerning whereas act with alternative nodes.

Ad hoc wireless networks reduce the limitations of substructure and permit strategies to generate and link nets on the fly-anytime, everywhere –for effectively any presentation.

II. RELATED WORK

Wireless networks are commonly higher susceptible and substantial safety intimidation than stable – wire line networks. The utilization of undefended and pooled announcement wireless channels revenues nodes with insufficient forcible safeguard and susceptible to security threats [4]. A MANET is a disseminated structure less arrangement, primarily confide on separate security resolution since every mobile node, as a consolidated security controller is tough to implement.

Security:

Security could be a vital module in essential set of connections like container furthering; direction-finding, set

Revised Manuscript Received on April 05, 2019.

Ms.D.Rajalakshmi, Research Scholar, Assistant Professor, Department of Computer Science and Engineering, Sri Sairam Institute of Technology, Chennai and Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R& D Institute of Science and Technology, Chennai, India.

Dr.K.Meena, Associate Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R& D Institute of Science and Technology, Chennai, India.

of connections utilize the merely threatened. If countermeasures to be mounted in the essential system, the tasks at the primary phases of the strategy. In wireless networks, essential tasks are supported by entire leaf nodes.

In network mechanism the undefended atmosphere, any node can threaten the consistency of the network utilities. The scourge are not impartial limited to maleficence, a fresh type of mischievousness termed as self-centeredness must take to avoid nodes do not collaborate. The safekeeping of connection is considerably tougher task. It stipulates the security comprising key administration, secure overwhelming protocols, collaboration, and intrusion discovery systems.

Finding and Avoiding Mischievous Nodes:

In radio communication the connections are multi directional and the exact probability is increased in Media Access Control layer protocols containing IEEE standard 802.11. The watchdog recognizes mischievous leaf nodes, pathrater ignore the overwhelming packets over to the leaf nodes [5]. When a leaf node onwards a packet, the leaf node's watchdog authorize and authenticates, the succeeding leaf node in the route also forwards the packet. The watchdog does this by promiscuously to the succeeding leaf node's transmission. If the succeeding leaf node does not onwards the packet, it is mischievous. The pathrater uses this mischievousness attentiveness to monitor the packet delivery.

Watchdog:

Fig.2 the watchdog technique employed to discover the mischievous nodes. Leaf node S transmits a data to the leaf node D. The leaf node A's transmission cannot be expected by leaf node C, it will listen the leaf node B's transportation. Once leaf node A transmits a data to leaf node B, predestined to leaf node C. Leaf node A could frequently convey if leaf node B again transmitting the previously sent the data. If the security process or cryptography is not completed separately for every connection, then the mobility leaf node A, convey the message to leaf node B has damaged with the data or the header.

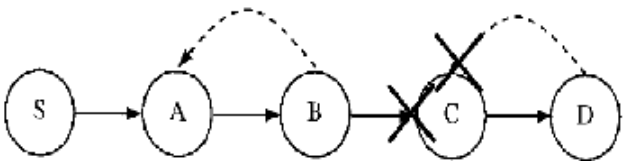

Fig.2. Watchdog Operation

Watchdogs are often enforced by conserving a buffer of data and comparing every snooped packet inside the buffer to outline if there's a match. If the data's are matched with the buffer, it removes the data from the buffer and it's not supervised by watchdog, so the data is forwarded to the destination. If the data's are not transferred in the specified time, watchdog intimated to the corresponding node through failure register notification and it's not forward the packets.

Advantage:

It discovers the misbehaving leaf nodes at the promoting level.

Weakness:

Watchdog not detecting the mischievous leaf nodes in the following circumstances [6]:

1. Confusing Collision
2. Receiver Crashing
3. Incorrect Misbehavior
4. Narrow Transmission Power
5. Several Colluding nodes
6. Partial Dropping

Confusing Collision: The confusing collision drawback avoids the snooping communications from various leaf nodes. Fig.2 elucidates, a packet collision arises at leaf node A and its wait for leaf node B to onward a packet. Here leaf node A is not knowing to figure out if the collision was pretentious by leaf node B's transmission, or if leaf node B never furthered and packet and the collision was pretentious by other leaf nodes in leaf node A's neighborhood. Based on this insecurity leaf node A, monitor the leaf node B activities for a period of time.

Receiver Crashing:

In the receiver crashing drawback leaf node A will solely convey the leaf node B, sends the packet to leaf node C, or it cannot convey if leaf node C receives it effectively. If a collision arises at leaf node C, leaf node B first onwards the packet. If leaf node A will solely outline, leaf node B has furthered the packet and admits that leaf node C has effectually received it. Here, leaf node B possibly skips the packet retransmission and escape discovery. This can be shown in fig.2.

Incorrect Misbehavior:

It happens when leaf nodes incorrectly report alternative leaf nodes as mischievous. A mischievous leaf node may attempt and divide the network by some leaf nodes path are mischievous. Fig.2 leaf node A report, leaf node B isn't forwarding packets once if truth be told it's completed. This may reason for leaf node S, sign the leaf node B as mischievous once if truth be told to leaf node A is the criminal. In the meantime leaf node A permits messages to the leaf node B, then acknowledgement from leaf node D to leaf node S can go from leaf node A to leaf node S. During the state of affairs, leaf node S may surprise the responses from leaf node D, once leaf node B is evidently falling information to the onward direction.

Narrow Transmission Power:

Mischievous nodes management its communication is avoided by watchdog. A leaf node bounds the broadcast power, such that the indication is robust adequate and its snooped by the preceding leaf node, it's too feeble for conventional to the correct receiver.

Several Colluding Nodes:

Several nodes collision will support an extra refined attack. For instance, leaf nodes B and C in Fig.2 may collide thus on reason of a mischief-person. During this case, leaf

node B frontwards information to leaf node C, however doesn't report back to leaf node A, once leaf node C drops the information. Based on this restriction, 2 sequential suspicious leaf nodes wouldn't be permissible during a routing path.

Partial Dropping:

Nodes may by-pass the watchdog by dropping packets at a lower rate than watchdogs expected mischievousness threshold. Watchdog won't discover the leaf node as mischievous; Due to these kinds of activities, leaf node is compulsorily onward to the defined data transmission rate. Based on this, watchdog works and implements the minimum information measure and figure out accurately. So, that watchdog must to identify wherever a packet ought between two hops.

The Ad hoc On-Demand Distance- Vector Protocol:

AODV offers quick, skillful direction and communication. AODV was thought-about exactly for ad hoc wireless networks, it delivers a communique between mobility nodes with insignificant overhead and minimal route attainment delay.

AODV does not decide to preserve ways from node to node with in the set of connections. Paths exposed to most required parameters and they are preserved in an essential manner. AODV is capable to deliver unidirectional, multi directional and broadcast communication capability. Merging all three communication forms in a particular protocol has lot of advantages. A protocol that deals both unicast and multicast communication efficient so that route information attained when examining for a multicast route can also improve unicast routing knowledge and vice versa. All three types of communication in a particular protocol make things easier coding. This basic algorithm will benefit both unicast and multicast data transmission [7].

AODV operates only symmetric links among adjacent nodes does not depend explicitly on individual aspects of the physical medium through which packets are distributed. AODV is proficient for operative on each wired and wireless media, though it's considered specifically for the wireless field [8].

Routing tables are employed by AODV to accumulate appropriate routing data. It exploits a unidirectional paths, & multi directional paths. This block is employed to accumulate the destination, next hop IP addresses and destination sequence number [9].

AODV reacts to topological alterations that disturb active routes in a speedy and timely manner. It constructs routes with only a lesser amount of overhead from routing control messages and no supplementary network overhead. AODV needs nodes to keep only next-hop routing information, thereby shrinking the storage prerequisite at each of the mobile nodes. To end with, AODV doesn't offer any additional difficulties on information packets since it doesn't deed the supply routing.

III. SYSTEM ARCHITECTURE

Intrusion discovery system accepts that employer and program activities are a unit noticeable, which implies that any action that the worker or an application programed and it get recorded where the initial arrangements of information and intrusion discovery systems has a straight forward approach to the organization records.

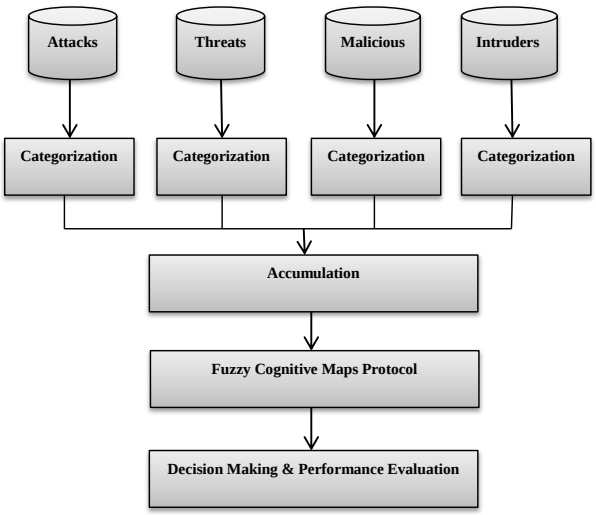

Fig.3 Intrusion Discovery System

This recorded system/employer connected information is termed as audit information. The intrusion discovery regards the capturing of auditing information, and these information evaluates either it's correct or not in a crucial aberration from standard organizational performance. Based on these kinds of problems advising a new protocol i.e., Fuzzy cognitive map protocol for distributing packets from source to destination in a secured fashion.

IV. PROPOSED SYSTEM

Fuzzy Cognitive Mapping:

Fuzzy Cognitive Maps realistically outline a system in to 2 basic elements: first one is, Perception Variables and another one is, Fundamental Associations. Nodes denote perception variables, P_x, where x is equivalent to one or it's up to N. A perception variable supplies the associative degree arrow it could be a source variable, where as a perception variable leads the termination or else the purpose of associative degree arrow is a result variable (or) impact variable [16]. The example of $P_h \longrightarrow P_i$, P_h is that the source variable that impacts P_i, which is the result variable.

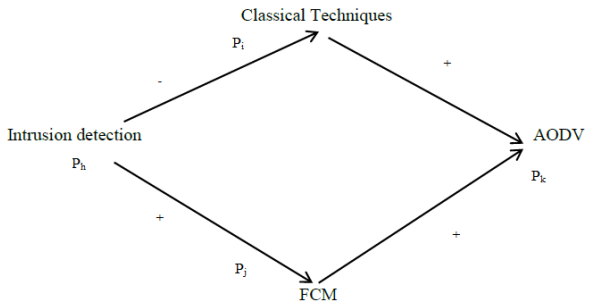

Fig.4 Conventional cognitive map for intrusion detection system

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Fig.4 denotes an easy cognitive Map, during which there are a unit contains, four perception variables (P_h represents Intrusion Detection, P_i represents the classical Techniques, P_k represents AODV concept and P_j represent the FCM concept).

Arrows denote the fundamental associations among perception variables; it may be positive or negative. As an example $P_h \rightarrow P_i$, P_h encompasses a negative fundamental association on P_i. Consequently, if P_h value increased means it leads to call P_i.

Path:

It represents two perception variables, P_h and P_k, denoted by P(h,k), All the nodes are coupled by an arrows from main node (P_h) to last node (P_k).

Cycle:

A Cycle is a route, it has associate degree arrow from termination point of route to the supply point of route.

Incidental Effect:

The incidental impact of route from source variable P_h to the impact variable P_k, is indicated by IE(h,k), is the product of fundamental associations that custom the trail, from source variable to impact variable. If route has an identical quantity of negative arrows, the incidental impact is positive. If the trail has an abnormal amount of negative arrows, the incidental impact is negative.

Complete Effect:

The complete impact of source variable P_h is the impact variable P_k, which is denoted by CE(h,k), is the combination of all the incidental impacts of all source variables to the impact variables. If all incidental effects are positive, the complete effect is positive; otherwise it's negative. If some incidental effects are positive and few are negative, the sum is indeterminate.

Indeterminacy:

The fundamental boundaries are biased with positive or negative floating point numbers, the incidental impact is, the product of every weight in the given path, and the complete impact is the summation of route products. This technique weights the route associations, it eliminates the difficultly of indeterminacy from the whole impact calculation. Additionally it needs a better performance of fundamental perception.

Fuzzy Cognitive Maps (FCMs):

It highlights the easy binary association of a CM required to be prolonged to comprise many degrees of rise or drop, then a fuzzy cognitive map (FCM) plays a vital role in intrusion discovery in MANETS. FCM encompasses, information of inevitable cognitive maps by allowing models, it denoted by linguistically with a completed fuzzy, instead of stringent to correct. FCMs are examined by geometrically or numerically.

Geometrical analysis is performed in small FCMs, whereas essentially it traces the growing and shrinking effects of all methods. Numerical analysis is performed in larger FCMs, whereas the models units are denoted by a fuzzy relational matrix, called an adjacency matrix [18].

Adjacency Matrix:

A Cognitive Map (CM) is altered employing a matrix known as adjacency matrix. Adjacency matrix is a square matrix it signifies the result of source variable (row) laid out in the CM has the result variable (Column). The subsequent matrix is an adjacency matrix for the CM. The adjacency matrix for a CM with k nodes uses an associate degree, i.e., k x k matrix, the associate degree entry within the (i,j) position of the matrix represents associate degree arrow between nodes P_h and P_i. Arrow shows in Fig.4 represents the "strength" of the result among the 2 nodes (i.e., a "+1" represents that the result is to rise, wherever as "-1" represents that the result is to drop).

$$Z = \begin{array}{c} \\ P_h \\ P_i \\ P_k \\ P_j \end{array} \begin{array}{c} \begin{array}{cccc} P_h & P_i & P_k & P_j \end{array} \\ \begin{bmatrix} 0 & -1 & 0 & +1 \\ 0 & 0 & +1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & +1 & 0 \end{bmatrix} \end{array}$$

Threshold Function:

Perception states, square measure the inside distinct boundaries through the threshold function. It defines the performance of a CM.

A bivalent threshold function needs the result of one or zero, which is such as "on" or "off":

$w(m_i) = 0, \quad m_i \leq 0$
$w(m_i) = 1, \quad m_i > 0$

The powerfulness threshold function includes negative activation. Therefore, ideas have a worth of one, 0 or -1 that is corresponding to "positive effect", "no effect and negative effect, etc.

$w(m_i) = -1, \quad m_i \leq -0.5$
$w(m_i) = 0, \quad -0.5 < m_i < 0.5$
$w(m_i) = 1, \quad m_i \geq 0.5$

Perception squares are measuring the fundamental association loads and result perception. Where, the square measures various kinds of attributes, to the relevant contribution:

$$M_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} PjLji$$

Where,
M_i = participation of Members
P_j = perception condition
L_{ji} = load of the fundamental associations

Evaluation:

In Fuzzy Cognitive Maps energetic systems, measure the cyclical and evaluation is performed inside the specific series. Every perception variable is an original price supported by the boldness of professionals about the present condition. The Fuzzy Cognitive Map is absolving towards

the stability is reached. Stability is outlined in future a new state vector will be a clone of a previous state vector.

V. EXPERIMENTS AND RESULTS

The Watchdog system fails to get discovers malicious misbehaviours occurred in these conditions: i) ambiguous collisions ii) receiver collisions iii) false misbehaviour iv) Transmission Power v) Multiple colluding nodes and vi) Partial dropping. During this section, estimate the performance of above circumstances of mischievous node actions are observed by the hybrid protocol using Fuzzy Cognitive Maps.

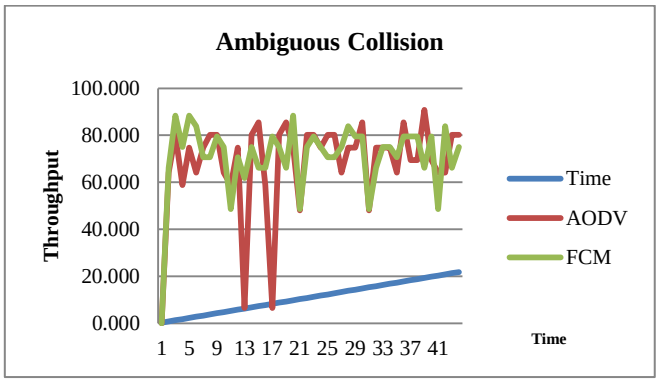

Fig.5 Ambiguous Collision

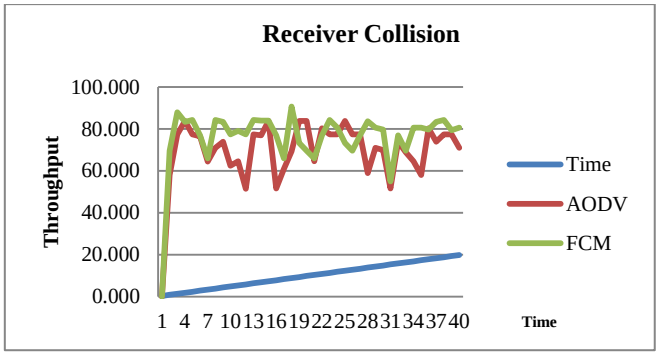

Fig.6 Receiver Collision

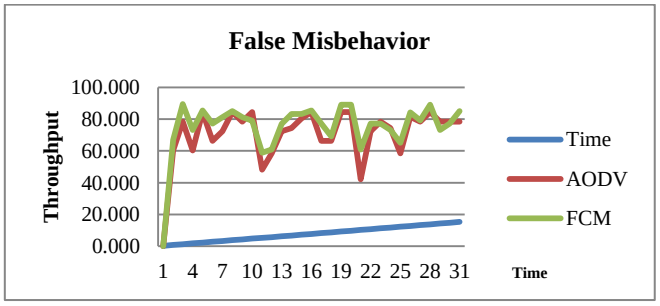

Fig.7 False Misbehavior

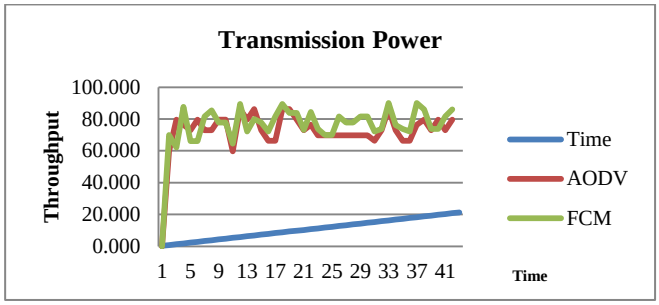

Fig.8 Transmission Power

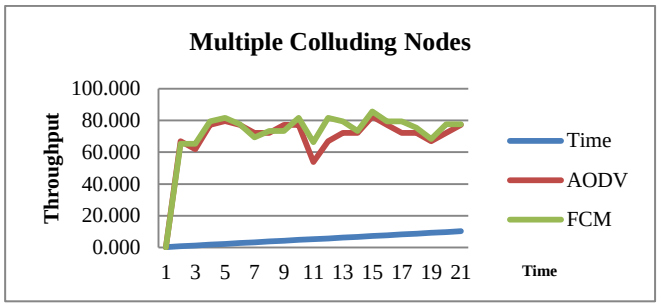

Fig.9 Multiple Colliuding Nodes

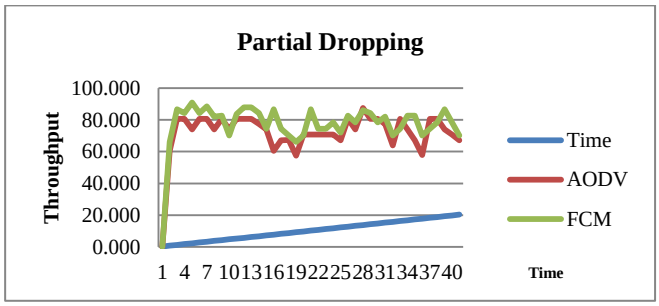

Fig.10 Partial Dropping

The act of imitating the behavior of some situation the model is characterized by good organization at intervals the Simulator (i.e) a machine that stimulates an environment for the purpose of training or research - NS 2.34 surroundings. It's to reinforce and evaluate the system behavior of results shows that different analysis works, it's a tendency to enforced the standard situation, the environment can be adjusted to operate in NS2.34.The demand to live environment and evaluate the structure of system to the subsequent 2 benefit oriented metrics are: 1.Packet Transmission rate, 2. Throughput in a pair of totally different protocols .i.e., AODV and FCM Protocol. With regard to the outcomes, we discover FCMs as an additional fascinating theme in MANETs.

VI. CONCLUSION

Wireless networks are progressively employed for circumstances where fixed set-up networks are not practical. In all times the intrusion prevention is not practical, so intrusion discovery is more essential in MANETs. Several methods are used in the direction of finding intrusions, specially Enhanced Adaptive Acknowledgement and AODV Protocol, but none of the approaches are infallible, and it is

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

doubtful that any will ever be, they all existing an improvement in the safekeeping position of MANETs. The watchdog is used in entire IDS, but here lot of limitations occurred. The watchdog was not worked accurately into the occurrence of collisions, it leads to incorrect indictment. The IDS could be intended to collaborate with those prevention techniques if they are adopted by the proposed Fuzzy cognitive maps protocol, which possibly will keep the IDS efficient and reduce the resource constraint; it discovers physical intrusion than on other protocols like AODV. This Fuzzy cognitive maps protocol is a robust system, incorporated mechanism for routing and data security.

REFERENCES

1 Ningrinla Marchang, Raja Datta and Sajal K.Das," A Novel Approach for efficient Usage of Intrusion Detection System in Mobile Ad hoc Networks", IEEE Transactions on Vehicular Technology, Vol.66,No.2,pp.1684-1695,2017

2 Francisco J. Aparicio-Navarro, Konstantinos G. Kyriakopoulos,Yu Gong, David J.Parish and Jonathon A. Chambers, "Using Pattern-of-life as contextual information for anomaly-based intrusion detection systems", IEEE Access,2017.

3 F. J. Aparicio-Navarro, K. G. Kyriakopoulos, D. J. Parish, and J. A. Chambers, ''Adding contextual information to intrusion detection systems using fuzzy cognitive maps,'' in Proc. IEEE Int. Multi- Disciplinary Conf. Cognit. Methods Situation Awareness Decision Support (CogSIMA), Mar. 2016, pp. 187–193.

4 S. Zeadally, R.Hunt, Y.S Chen, A. Irwin and A.Hassan, "Vehicular ad hoc networks (VANETS): Status, Results, and challenges," Telecommunication Systems, Vol.50, no.4, pp.217-241, 2012.

5 Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic. Data-centric misbehavior detection in vanets. ArxivarXiv:1103.2404v1, 2011.

6 R. H. Akbani, S. Patel, and D. C. Jinwala, ―DoS attacks in mobile ad hoc networks: A survey,‖ in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

7 F. Abdel-Fattah, Z. Md. Dahalin, S. Jusoh, Dynamic intrusion detection method for mobile ad hoc networks using CPDOD algorithm, International Journal of Computer Applications, vol. 2, Published by the Foundation of Computer Science, 2010. pp. 22–29.

8 K. Stanoevska-Slabeva and M. Heitmann, ―Impact of mobile ad-hoc networks on the mobile value system,‖ in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2010

9 R. Akbani, T. Korkmaz, and G. V. S. Raju, ―Mobile Ad hoc Network Security, in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

10 Elhadi M.Shakshuki, Nan Kang and Tarek R.Sheltami, EAACK – A Secure Intrusion Detection System for MANETs‖ in Industrial Electronics, Vol 60, No.3, 2013.

11 D.Rajalakshmi,K.Meena, "A Survey of intrusion detection with higher malicious misbehavior detection in Manet", International journal of civil engineering and technology, Vol.8, 2017.

12 S. Banerjee, C. Grosan, A. Abraham, P.K. Mahanti, Intrusion detection on sensor networks using emotional ants, International Journal of Applied Science and Computations 12 (3) 152–173, 2005.

13 Dharmendra G. Bhatti, P. V. Virparia, Bankim Patel,Data Pre-processing for Reducing False Positive Rate in Intrusion Detection, International Journal of Computer Applications (0975 – 8887) Volume 57–No.5, November 2012.

14 Yi P., Hou Y.F., Zhong Y., Zhang S., Dai Z.: Flooding Attack and Defence in Ad hoc Networks. In: Systems Engineering and Electronics, Vol. 17, No. 2, pp. 410-416 2006.

15 Mainak Ghosh, Anitha Varghese, Arobinda Gupta, Arzad Alam Kherani, and Skanda N. Muthaiah. Detecting misbehaviors in vanet with integrated root-cause analysis. Ad Hoc Networks, 8(7):778–790, 2010.

16 Syeda Gauhar Fatima, Dr. Syed Abdul Sattar and Dr. K. Anita Sheela, Energy Efficient Intrusion Detection System for Wsn, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 3, Issue 3, 2012, pp. 246-250.

17 S. Bueno and J. L. Salmeron, ''Benchmarking main activation functions in fuzzy cognitive maps,'' Expert Syst. Appl., vol. 36, no. 3, pp. 5221–5229,2009.

18 T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," Wireless/Mobile Network Security,Springer, 2006.

19 C. D. Stylios and P. P. Groumpos, ''Modeling complex systems using fuzzy cognitive maps,'' IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 34, no. 1, pp. 155–162, Jan. 2004.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication