International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Efficient AODV based MANET System with Fuzzy Logic Intruder Detection

Diksha Tripathi, Sumit Kumar Gupta, Ankur Shukla
Electronics and Communication Engineering,
Bansal Institute of Technology, Lucknow, India,
tripathidiksha2308@gmail.com, er.guptasumit@gmail.com, ankurs8886@gmail.com

Abstract: The work is a way to deal with identify malevolent hubs by applying fuzzy rationale in Mobile adhoc systems. Security is a noteworthy worry in different situations of adhoc sensor system. Identification of malignant hubs frames a fundamental piece of a way to deal with security. The proposed work utilizes fuzzy rationale to recognize the assault and noxious conduct of hubs. The proposed work will recognize the assault over the system and in addition give the answer for lessen the execution time over the system. The goal of the work is to give security in Mobile Adhoc Network. The proposed work utilizes AODV calculation. This calculation infers some fuzzy standards which is actualized on the hubs in the system.

Keywords—Routing protocols, Optimization Network, Metaheuristics Optimization, Path loss, quality of service.

1. Introduction:

Mobile Ad hoc NETworks (MANET) are the wireless networks of mobile computing devices without any support of a fixed infrastructure. The mobile nodes in a MANET self organize together in some arbitrary fashion. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. These networks can be applied between persons or between vehicles in areas which are depleted of fixed infrastructure. Two nodes can directly communicate with each other if they are within the radio range. If the nodes are not within the radio range they can communicate with each other using multi hop routing. The wireless link between the nodes in mobile networks is highly vulnerable. This is because nodes can continuously move causing the frequent breakage of the link. The power available for transmission is also strictly limited. The topology of the network is highly dynamic due to the continuous breakage and establishment of wireless link Nodes continuously move into and out of the radio range. This gives rise to the change in routing information. The network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves i.e. routing functionality will be incorporated into mobile nodes. MANET is more vulnerable than wired network due to mobile nodes, threats from malicious nodes inside the network. Because of vulnerabilities, MANET is more prone to malicious attacks. MANET has following vulnerabilities.

2. Related Work:

Yogita Danane, and Thaksen Parvat, (2015) [1] according to them PC security has turned into an imperative piece of the day today's life. Single PC frameworks as well as a broad system of the PC framework additionally requires security. In accomplishing the security of the frameworks, an Intrusion Detection System (IDS) assumes a huge part. IDS is a product that screens the PC arrange and identifies the suspicious exercises that happen in the frameworks or system. The procedure of interruption identification incorporates recognizing interruption. Interruption is a suspicious action endeavored by the aggressor. This work shows a fluffy hereditary way to deal with distinguishing system interruption. Work displays the aftereffects of the proposed framework regarding precision, execution time, and memory designation. To execute and measure the execution of the framework the KDD99 benchmark dataset is utilized. The KDD99 dataset is a benchmark dataset that analysts use in different system security explores. Hereditary calculation incorporates an advancement and gathering that uses a chromosome like information structure and add to the chromosomes utilizing determination, hybrid and change administrators. Fluffy guideline sorts system assault information.

Salma Elhag, Alberto Fernández, Abdullah Bawakid, Saleh Alshomrani, and Francisco Herrera (2015) [2], they worked on the security approaches of data frameworks and systems that are intended for keeping up the honesty of both the secrecy and accessibility of the information for their trusted clients. Then again, various malignant clients break down the vulnerabilities of these frameworks keeping in mind the end goal to increase unapproved access or to trade off the nature of administration. Thus, Intrusion Detection Systems have been outlined keeping in mind the end goal to screen the framework and trigger alarms at whatever point they discovered a suspicious occasion. Ideal Intrusion Detection Systems are those that accomplish a high assault discovery rate together with a little number of false cautions. Be that as it may, digital assaults present a wide range of qualities which make them difficult to be appropriately distinguished by straightforward factual systems. As indicated by this, Data Mining methods, and particularly those situated in Computational Intelligence, have been utilized for actualizing strong and exactness Intrusion Detection Systems. In this work, we consider the utilization of Genetic Fuzzy Systems inside of a pairwise learning structure for the advancement of such a framework. The benefits of utilizing this methodology are twofold: to start with, the utilization of fluffy sets, and particularly semantic marks, empowers a smoother fringe between the ideas, and permits a higher interpretability of the

All Rights Reserved © 2024 IJRDASE

standard set. Second, the separation and-vanquish learning plan, in which we differentiate all conceivable pair of classes with points, enhances the accuracy for the uncommon assault occasions, as it gets a superior distinguishableness between an "ordinary movement" and the diverse assault sorts. The integrity of our technique is upheld by method for a complete trial study, in which we differentiate the nature of our outcomes versus the best in class of Genetic Fuzzy Systems for interruption location and the C4.5 choice tree.

The work entitled “Fuzzy Logic based Intruder Detection System in Mobile Adhoc Network” by **Shadab Siddiqui, P. M. Khan and Muhammad Usman Khan (2014) [3],** is an approach to detect malicious nodes by applying fuzzy logic in Mobile ad-hoc networks. Security is a major concern in various scenarios of adhoc sensor network. Detection of malicious nodes forms an essential part of an approach to security. The proposed work uses fuzzy logic to identify the attack and malicious behavior of nodes. The proposed work will identify the attack over the network as well as provide the solution to reduce the execution time over the network. The objective of the work is to provide security in Mobile Adhoc Network. The proposed work uses AODV algorithm. This algorithm implies some fuzzy rules which is implemented on the nodes in the network. The if-then rules of fuzzy will identify the malicious node in the network. The proposed work will do comparison between the performance parameters obtained from AODV with priority based Intruder detection system with AODV implementing fuzzy logic to identify malicious nodes. The results will show great improvement of AODV with fuzzy logic over the previous algorithm. The proposed scheme is implemented using Matlab & its results show its effectiveness.

3. Methodology:

Intrusion Detection System (IDS) has become a primary study area in Computer-based security. It is a well-known skill for enlightening and is used to protect data consistency and system accessibility throughout an intrusion. When a person tries to access an information structure in the system or does any illegal action, the action is known as an intrusion that further has two types, exterior, and interior. The exterior are those people who do not have authority to access the system information and still they try to obtain illegitimately with the help of different saturation techniques. While interior is those who have a legal permission to access system, but try to do illegal activities. Software bugs exploitation and miss configurations of the system cause intrusion. Sniffing unsecured traffic, password cracking, or utilizing the particular protocols design flaw are also some of the ways that cause intrusion.

Any information system should accomplish three main principles for guarantee a correct access to the data, namely confidentiality, integrity and availability. Unfortunately, all networks could be the object of unauthorized accesses so that a strong security policy must be established for avoiding this violation of the prior principles [14]. The technology developed for this aim is known as IDS, which dynamically monitors logs and network traffic, applying detection algorithms to identify these potential intrusions within a network [13]. In particular, IDS can be split into two categories according to the detection methods they employ, including (1) misuse detection and (2) anomaly detection.

Misuse detection systems use an established set of known attack patterns, and then monitor the net trying to match incoming packets and/or command sequences to the signatures of known attacks [22]. Hence, decisions are made based on the prior knowledge acquired from the model. Starting from a wide collection of cyber-attacks results in an extremely efficient system, comprising low false alarm rates. Additionally, the system administrator could reliably determine which attacks the system is experiencing immediately upon installation. This fact is the main advantage and, at the same time, the main drawback of this kind of system: maintaining a database for all of the possible attacks against a network is a tedious, if not impossible task in a modern computer network environment, limiting its accuracy when faced with the challenge of detecting new intrusive activities.

Proposed work:

The proposed work consists of four phases namely Path generation using AODV algorithm, applying Fuzzy logic, verification and detection of malicious nodes.

Phase One: Path generation using AODV algorithm

In this phase AODV algorithm is applied to generate path for route discovery. AODV uses all its features to generate the path from source to destination.

Phase Two: Applying Fuzzy logic

In this phase the generation of fuzzy rules takes place along with membership function. The fuzzy IF-THEN rules are applied in order to detect malicious node.

Phase Three: Verification

In this phase verification of IF-THEN rules takes place. The condition of IF statement verified by checking if the destination sequence number is much greater than source sequence number and if response time of node is greater than set threshold value then malicious node is detected

Phase Four: Detection of malicious node

In this phase we will be able to detect the malicious node by applying fuzzy rules.

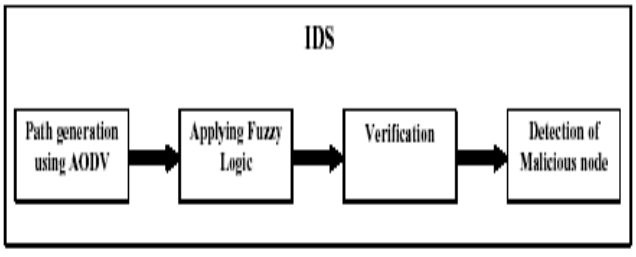

Fig 1: Proposed Fuzzy based IDS

4. Result and Discussion:

It is the time used by algorithm for execution

All Rights Reserved © 2024 IJRDASE

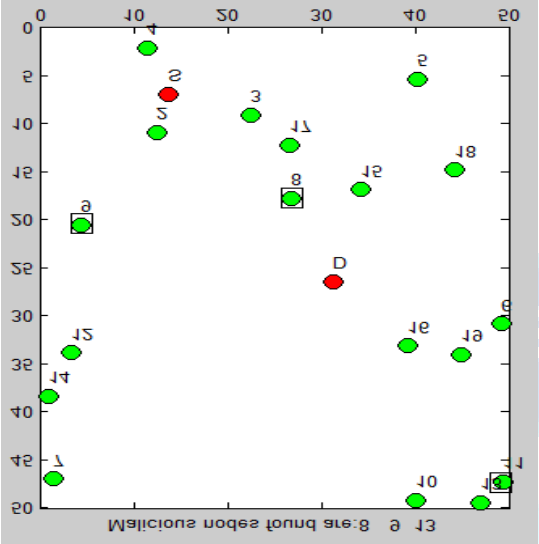

Figure 2: Displaying malicious nodes for a network distribution in 50*50 area

Figure 2 shows the nodes of a MANET system distributed randomly in an area of 50x50 m area field. The S is the source node and it has to send data packet to destination D. In this case the routing system applies the fuzzy logic rules to detect the MALICIOUS node and it is shown in figure the malicious node that are found here has id 8, 9 and 13 for present MANET status. Hence the proposed algorithm will reject the detected malicious nodes and thereafter applies the AODV protocol for establishing the route between S to D nodes.

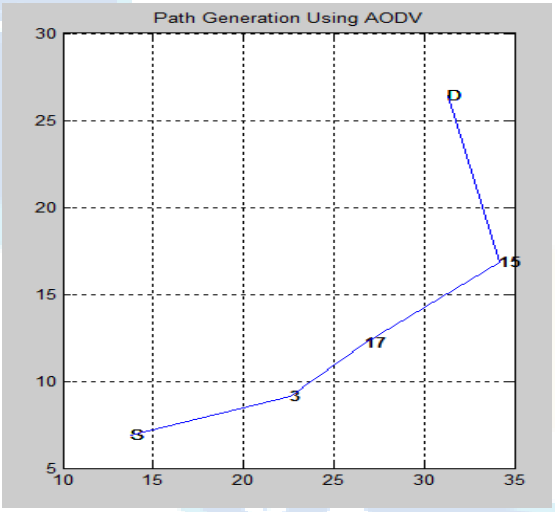

Figure 3a: Line showing path from source to destination

The nodes that are selected for the developed path are connected the show the determined route from source to destination as shown in figure 3 a. We can see that the selected path is going [S 3 17 15 D] for the network shown in figure 1.

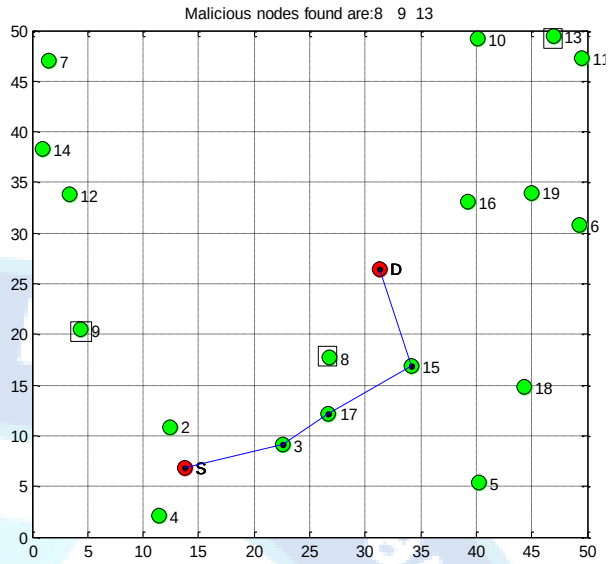

Figure 3b: Path from source to destination

Figure 3 b shows the data transmission over the network along with the detected malicious nodes. It is evident that none of the malicious node is considered in the selected path developed by AODV routing modified search in hybrid of fuzzy logic rules.

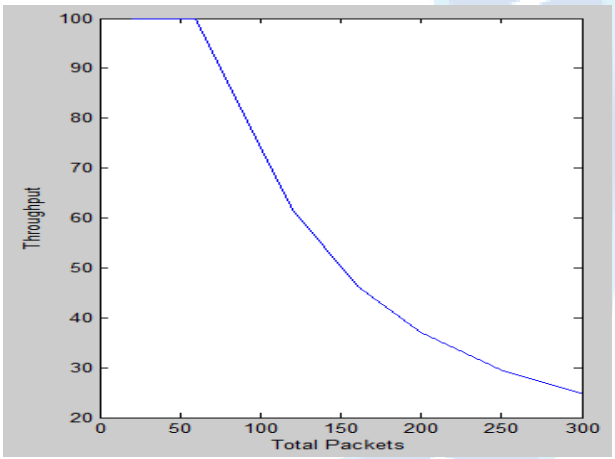

Figure 4: Graph displaying throughput

5. Conclusion:

The security of MANET has picked up ubiquity among examination region. The security issues are examined and we have dissected the security framework with our proposed model Intruder Detection System in MANET utilizing Fuzzy Logic. This model is extremely effective for securing against assaults. Our proposed model can locate the protected course and offers in identifying so as to keep some assistance with attacking in MANET the hub with succession no and limit esteem.

References:

[1] Yogita Danane, and Thaksen Parvat, "Intrusion Detection System using Fuzzy Genetic Algorithm", 2015 International Conference on Pervasive Computing (ICPC).

[2] Salma Elhag, Alberto Fernández, Abdullah Bawakid, Saleh Alshomrani, and Francisco Herrera, " On the combination of genetic fuzzy systems and pairwise learning

All Rights Reserved © 2024 IJRDASE

for improving detection rates on Intrusion Detection Systems" Expert Systems with Applications 42 (2015) 193–202.
[3] Shadab Siddiqui, P. M. Khan and Muhammad Usman Khan, "Fuzzy Logic Based Intruder Detection System in Mobile Adhoc Network" BIJIT - BVICAM's International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA) (2014)
[4] B.Ben Sujitha1, R.Roja Ramani2, Parameswari: Intrusion Detection System using Fuzzy Genetic Approach; International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 10, December 2012.
[5] Devendra K. Tayal, Amita Jain and Vinita Gupta "Fuzzy Expert System for Noise Induced Sleep Disturbance and Health Effects" in BIJIT Issue3: (Jan-June 2010 Vol2 No1).
[6] Bharanidharan Shanmugam and Norbik Bashah Idris,"Improved Intrusion Detection System using Fuzzy Logic for Detecting Anamoly and Misuse type of Attacks" 2009 International Conference of Soft Computing and Pattern Recognition.
[7] Elmar Gerhards-Padilla, et.al." Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", 32nd IEEE Conference on Local Computer Networks 0742-1303/07© 2007 IEEE.
[8] Zaheeruddin, Vinod K. Jain, and Guru V. Singh , "A Fuzzy Model For Noise-Induced Annoyance", IEEE transactions on systems, man, and cybernetics –Part A: Systems and Humans, Vol. 36(No. 4), July 2006.
[9] X. Wang, T. Lin and J. Wong, "Feature selection in intrusion detection system over mobile ad-hoc network," Technical Report, Computer Science, Iowa State University, 2005.
[10] Sampada Chavan, Neha Dave and Sanghamitra Mukherjee "Adaptive Neuro-Fuzzy Intrusion Detection Systems" Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) 0-7695-2108-8/04 $ 20.00 © 2004 IEEE
[11] Jakob Jonsson and Burton S. Kaliski Jr., " On the Security of RSA Encryption in TLS" published in 2002.
[12] Scott Fluhrer et. al. , " Weaknesses in the Key Scheduling Algorithm of RC4", Springer-Verlag Berlin Heidelberg 2001.
[13] Axelsson, S. (1998). Research in intrusion-detection systems: A survey. Technical Report 98–17, Department of Computer Engineering, Chalmers University of Technology, Goteborg.
[14] Chebrolu, S., Abraham, A., & Thomas, J. P. (2005). Feature deduction and ensemble design of intrusion detection systems. Computers and Security, 24(4), 295–307.
[15] Sourav Sen Gupta et. al., " Dependence in IV-related bytes of RC4 key enhances vulnerabilities in WP" IACR 2014.
[16] Sourav Sen Gupta et. al., " Proof of Empirical RC4 Biases and New Key Correlations", Published in 2012.
[17] Nidhi Singhal, and J.P.S.Raina, " Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011.
[18] Pouyan Sepehrdad et. al., " Discovery and Exploitation of New Biases in RC4", Published in 2011.

All Rights Reserved © 2024 IJRDASE