AODB Protocol using Fuzzy Logic

Sakshi, Madan Kushwaha
Computer Science and Engineering,
Bansal Institute of Engineering and Technology, Lucknow, India.

Abstract: In this paper proposed an approach in which the aim is to find the method for authentication which is more energy efficient and reduces the transmission time of the network. MANETs are of dynamic topology and have no predefined infrastructure. Due to its dynamic topology this network is prone to various kinds of vulnerable attacks. Sensor networks are battery operated and is a major concern. Methods on ID based Authentication consumes more network bandwidth and increases the computation and transmission time of the network. So for better operation, authentication must be the major factor of concern. In this paper a method for authentication in adhoc sensor network is proposed which is based on certificate based security services. Here we will make use of X.509 certificate format. In this some modification is made to the certificate format such that the transmission time and energy consumption of the network is reduced. The certificate is deployed on all nodes before starting the communication. The hashing algorithm SHAI is used to calculate the hash of these certificates .The X 509 certificates is issued by a certification Authority (CA)and is encrypted using private key of CA. The algorithm used for encryption of hash codes in RSA which uses public and private keys of CA. If two nodes wish to communicate then decryption is done .The decryption is done using public key of CA.

Keywords: AODB protocol, MANET, Fuzzy Logic, RSA

1. Introduction:

Mobile Adhoc 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.

- **Lack of centralized node:** MANET doesn't have a centralized node. The lack of centralized makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale adhoc network.
- **Resource availability:** Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self organized security mechanism.
- **Scalability:** Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.
- **Dynamic topology:** Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.
- **Limited power supply:** The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.
- **Bandwidth constraint:** Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.
- **Adversary inside the Network:** The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.
- **No predefined Boundary:** In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node.

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 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.

B.Ben Sujitha, R.Roja Ramani, and Parameswari (2012), [4] according to them system security is of essential concerned now days for huge associations. The interruption discovery frameworks (IDS) are getting to be vital for viable security against assaults that are continually changing in extent and multifaceted nature. With information trustworthiness, secrecy and accessibility, they must be solid, simple to oversee and with low support cost. Different adjustments are being connected to IDS frequently to distinguish new assaults and handle them. This work proposes a fluffy hereditary calculation (FGA) for interruption location. The FGA framework is a fluffy classifier, whose learning base is displayed as a fluffy govern, for example, "if-then" and enhanced by a hereditary calculation. The strategy is tried on the benchmark KDD'99 interruption dataset and contrasted and other existing strategies accessible in the writing. The outcomes are empowering and exhibit the advantages of the proposed approach.

Devendra K. Tayal, Amita Jain and Vinita Gupta (2010) [5], in their work an exertion has been made to add to a fluffy based model to think about the effect of different clamor components on Sleep unsettling influence and Health. We altogether overview the current writing and distinguish the inadequacies in the current models in this field. We then distinguish different commotion elements which can have the huge effect on Sleep and wellbeing. The MIMO Expert framework created in this work gives rest aggravation, wellbeing condition in the morning and wellbeing as yield variables and clamor level, short commotion span, long clamor length of time, age and Type of commotion as the data variables. Fitting fuzzification and defuzzification techniques have been utilized and the usage as a part of MATALAB 7.0.1 has been finished. It has been built up from work of different specialists that impact of important commotion like tunes and talks influence rest and wellbeing conditions severely than aimless clamor like railroad clamor, roadside commotion. Essentially other info variables influence rest and wellbeing condition. These variables have been concentrated on in this work. The commotion level and length of time of clamor, which are likewise the conspicuous components in choosing impact on listening to yield variable have been talked about, for e.g. a commotion of low level does not have noticeable influence on person starting abnormal state of clamors.

3. Intrusion Detection System

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.

On the contrary, anomaly detection methods seek to overcome this problem by defining a ‘‘normal’’ behavioral model, and assuming that any deviation from this profile is considered to be an attack [23]. Therefore, good detection results can be obtained from novel attacks. Additionally, learned profiles of normal activity are customized for every system, making it quite difficult for an attacker to know with certainty what activities it can carry out without getting detected. However, anomaly detection systems also present several technical challenges. First of all, the complexity of developing a system of these characteristics is higher than in the case of misuse detection. Furthermore, a higher percentage of false alarms are raised, together with the problem of accurately determining which kind of alarm has been triggered.

3.1 IDS Terminology:

1) Alert/Alarm- It is a signal signifying that the system already been or is being attacked.
2) True Positive- It is an applicable attack which initiates IDS to make an alarm.
3) False Positive- It is an action signaling IDS to make an alarm when there is no attack taken place.
4) False Negative- It is a breakdown an IDS to become aware of a real attack.
5) True Negative- When no attack has taken place IDS does not make any alarm.
6) Noise- It is Data or intrusion that can initiate a false positive.
7) Site policy- Guiding principles of an institute those used to manage the system and configurations of IDS.
8) Site policy awareness- It is the capability of an IDS to modify its policies and configurations vigorously according to the changing environmental activity.
9) Confidence value- It is a value an institute gives to an IDS based on past presentation and study to help conclude its capability to recognize a threat efficiently.
10) Alarm filtering- It is a method of sorting attack alerts available from an IDS to differentiate false positives from real attacks.

Proposed Work:

The characteristics of MANET such as dynamic topology & energy constrained operation are a challenging issue. Security is also an important issue in the field of MANET. Security leads to authentication among nodes. Many methods have been proposed to provide security & authentication among nodes in MANET. In our work we will make use of X.509 authentication certificate format. We will modify the certificate format such that the size of certificate is reduced thereby leading to reduction in transmission time & energy consumption. This system will make use of RSA algorithm for encryption and SHA-1 logic for hashing

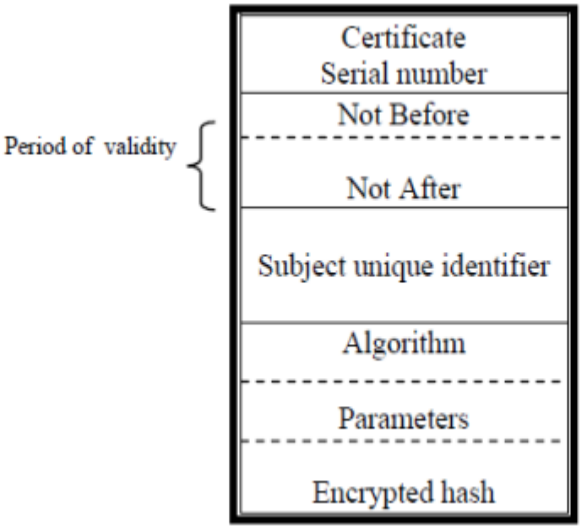

Fig 1: The (X.509 M) Certificate

In our proposed certificate the fields which are taken are as follows:-

- **Serial number:** It is an integer value unique within the issuing CA that is associated with the certificate.
- **Period of validity:** It consists of two dates: the first and last date on which the certificate said to be valid.
- **Subject unique identifier:** It is a bit string field which optional and is used to identify uniquely the subject.

- **Signature:** It covers all the fields of the proposed certificate. It also contains the hash value of all the other fields and encrypted with the CA (Certification Authority) private key. This field includes the signature algorithm identifier.

4. Result and Discussion:

Here we will evaluate our model Intruder Detection system in MANET. This system is developed to operate anywhere in any situation, therefore the experiment is carried out with same scenario with different experiments that shows the performance of system. The parameters used for simulation will be compared to the existing model.

It is very important to choose suitable parameters for system evaluation. The performance parameters will describe the result of simulation. These parameters are important as they will be used to notify what will actually happen during simulation

Our choice is using MatLab- 2010. Matlab uses the hierarichal architecture in order to define components like nodes & network. The components are defined by text based language. The components can be nested to form complex module inside each other.

Every module can be accomplished by C++ file which describe its behavior. MatLab provides many modules such as queues, tools etc. by using C++ computation. MatLab uses documentation & active discussion forums.

Here we will evaluate our model Certificate based security services in Adhoc Sensor Network. The parameters used for simulation will be compared to the existing certificate. It is very important to choose suitable parameters for system evaluation. The performance parameters will describe the result of simulation. These parameters are important as they will be used to notify what will actually happen during simulation. MatLab- 2010 will be used as simulation tool because Matlab uses the hierarchal architecture in order to define components like nodes & network

Table 1: Measurement of MATLAB

The experiments were carried out by MatLab-2010. The scenarios developed to carry out the tests use as parameters the mobility of the nodes and the number of active connections in the network. Node are presented previously were utilized in the experiments. The choices of the simulator are presented in table 1	Matlab-2010
Simulation Area	100*100m
No of nodes	10 to 100
Transmission range	25m
Mobility Model	Random Waypoint
Max Speed	5-20 m/sec
Traffic Type	CBR(UDP)
Data payload	1500 bytes
Packet rate	2 packet/sec
Sensor type	Crossbow MICA2DOT mote.
Simulation time	30 sec
MAC	802.11
Pause Time	20 sec
Mobility	10.70 m/s
Terrain area	100*100m

4.1 Validation in terms of metrics used for comparison

In this section we will validate our thesis by comparing modified & original certificate based on various parameters. The sensor used for validation is Chipcon CC1000 radio in Crossbow MICA2DOT mote.

4.1.1 Energy Consumption in transmission & reception

E s= (Etx E) r= (E Where, rx) Etx E –It is the energy required to transmit a byte. Rx Here we will calculate the energy consumption due to transmission/reception of varying certificate sizes. It is the energy required to receive a byte. The energy consumption in transmission of 1 byte is 28.6 µJ [4] respectively. The energy consumption in reception of 1 byte is 59.2 µJ [4] respectively. For proposed certificate the size is of 31 bytes, therefore total energy associated with proposed certificate in transmission is 886.6 µJ and 1835.2 µJ in reception respectively. The original size of X.509 certificate is of 82 bytes; therefore total energy associated with proposed certificate in transmission is 2345.2µJ and 4854.4µJ in reception respectively.

4.1.2 Energy consumption on computation

Here we will calculate the computation overhead of the proposed schemes in terms of energy consumption. The energy consumption in 1 byte of computation is 7.6mJ respectively [4]. For proposed certificate the size of 31 bytes requires energy consumption as 235.6 mJ. The original size of X.509 certificate is of 82 bytes; therefore total energy associated with proposed certificate is 623.2 mJ.

4.1.3 Transmission time

It is the amount of time from beginning till the end of message transmission. The cost of 1 byte in transmission is 8.8*10-4 msec [6] respectively. Therefore the transmission cost associated with total size of proposed certificate is 2.728*10-2 The cost associated with 82 bytes of original certificate is $7.216*10^{-2}$.

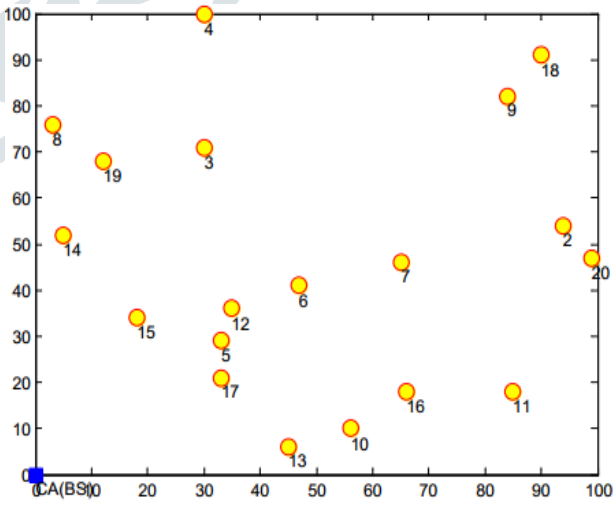

Fig 2: Displaying no of nodes in 100*100 area with CA

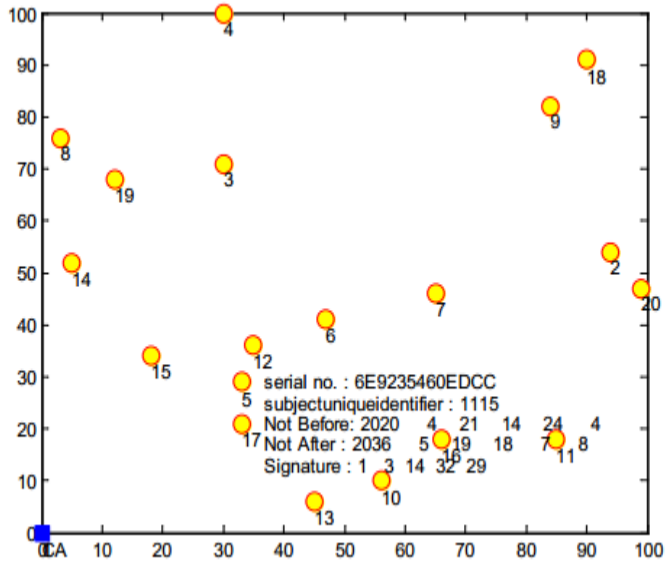

Fig 3: Displaying certificate of a specified nodes

5. Conclusion:

Here we have made use of X.509 certificate format. In this some modification is made to the certificate format such that the transmission time and energy consumption of the network is reduced. Our proposed model will provide authentication among nodes and security in MANET. The proposed work is implemented in MATLAB and the result will show the effectiveness of proposed certificate in MANET. The proposed work will initially reduce the size of original certificate which is then deployed among nodes in MANET by CA (Certification Authority) before starting the communication . Then the size of proposed certificate is taken .This size is taken as input to calculate the hash of the certificate by using SHA-1 hashing algorithm. The hash codes of the each node are then encrypted by using RSA algorithm. The key used for encryption is CA's private key and key used for encryption is CA's public key .Therefore all the nodes will store the encrypted certificate among them before transmission .Moreover if the two nodes wish to communicate then decryption is done at receiver at receiver node .If the match occurs then node is said to be authentic.

Reference:

[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 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.