iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review on Security Goals Requirements for the Manets

Er. Hemant Sharma[1] Er. Navneet Kaur[2]
[1]Scholar M. Tech (CSE)GIMET (PTU) Amritsar, India
[2]AP (CSE) GIMET (PTU)Amritsar, India

Abstract: ***Ad hoc networks are the most prominent field among the researchers to conduct the research in order to provide a solution to the main issue regarding the security of the data that is transferred over the network. As the data follows a particular route for reaching to the destination node and the route creation is done by inter-connecting the most adjacent nodes. In the techniques that ensure security for the transmission of data the emphasis was laid on the reputation of the nodes. In these techniques first the reputation of the nodes is checked and the selection of the route is done. After the selection of the route, the reputation of the each node is updated. This study provides a review to the trust based security mechanism to the data plane in the network which is capable to detect the malicious node that causes to the packet dropping in the network while communication process and also provide a brief presentation of fuzzy interference system.***
Keywords: Ad Hoc Networks, MANETs, VANETs, Trustworthiness, Security, Fuzzy interference system.

I. INTRODUCTION

Ad Hoc Networks are the wireless networks which poses the property of self organizing or did not follow any physical infra to settle down in the environment. Nodes or hubs in specially appointed systems (Ad Hoc Networks) act as both client and router. A few uses of specially appointed systems could incorporate mechanical and business applications including helpful versatile information exchange [1],such as military and protect operations. As of late, developing advances, for example, remote sensor systems (WSNs), wearable computing, pervasive processing, Internet of Things, have a great extent added to a further push toward application possibilities of specially appointed systems [2]. Ad hoc Networks present the characterized attributes of open connect, dynamic topology, and dispersed operation.

Ad hoc Networks are considered as totally self-ruling remote brief systems built up utilizing the gathered mobile devices principally for military, crisis and emergency situations, where no framework is accessible [3]. It is a gathering of versatile hubs which don't require a physical infrastructure or existence of the network for security and convenient purpose [4]. Likewise wireless or remote connections are powerless to connection assaults going from inactive listening in to dynamic meddling [5]. Dissimilar to hardwired systems with physical guard at firewalls and entryways, assaults on systems can originate from all headings and may focus on any node. Independent nodes have deficient physical assurance and can be caught, traded off, and captured effortlessly [6]. Interruptions from a compromised hub are more hazardous and significantly harder to recognize [7]. Harm incorporates releasing confidential data, intrusive message and imitating nodes or hubs, in this way violates the essential security necessities. All these imply that each hub must be set up to experience with a foe either directly or indirectly [8].

II. SECURITY GOALS

Security is the most imperative issue for the wireless networks from last few years specifically in real time based applications [9]. To make an ad hoc network secure from vulnerable interruption there are some characteristics that are required to remember.

A. Availability

is a property which defines that the network can be capable to work even in the state of denial of service attack. This attack can take place at any layer of the wireless ad hoc networks [10]. On MAC and physical layer an attack can leads to the traffic on the transfer media or channel whereas on network layer this attacks can leads to the disconnection of the network.

B. Confidentiality

depicts that the specific information will never be released to the unauthorized person or node. The deliberate or strategic

information like military data need to be keeping secure or confidential from enemy or third party [10]. If this kind of information is leaked or revealed to the third party then it can lead to the overwhelming consequences. The concept of confidentiality also mandatory to applicable on the routing information because the routing information can also proved beneficial for the enemies or intruders in order to locate their target in war.

C. Integrity

refers that the transferred message will never be corrupted and will remain reliable till it reaches to the destination [10]. The message or data can get corrupted due to malicious attacks on the network in order to have an unauthorized access to the information.

D. Authentication

depicts that the node which is indulged in routing has an authentic identity. An unauthentic node is prone to the errors or attacks since the adversary can access an unauthentic node easily and can gain access to the whole data [11]. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

E. Non-repudiation

is properties that have the capability to detect the non-repudiate nodes in the network and also broadcast a message in the network to the each node regarding the warning of repudiate node [12]. For example if node B sends a incorrect message to the node A then the property of non repudiation allows the node A to accuse the node B by sending an message and also broadcast this message over the network in order to persuade other nodes that the node B is compromised.

III. ATTACKS TO DATA PLANE

Attacks in the ad hoc network are mainly categorized in two types i.e. Active Attacks and Passive Attacks. In active attack the certified or authorized node performs the data tempering whereas in passive attack the unauthorized node gains the access over the data without interrupting the networking operations [13]. Another form of classification of attacks divides the attacks in two categories as internal attack and external attack. The internal attack refers to the form of attack where the attacker node related to the network whereas in external attack the attacker node is from outside the network. Internal attacks are considered to be more rigorous as compare to the external attacks because in internal attack the victim nodes have all the access to the confidential information [14]. Various security issues in form of attacks such as worm hole attacks, grey hole attack, Denial of Service attacks etc had been studied in past [15].

The data over the ad hoc networks can get infected if any of the following attack occurs in the network. There attacks are categorized in 4 parts as follows:

A. Black hole Attack

A black hole attack [14] [16] provides a shortest path of a destination node having a packet that a malicious node sends erroneous routing information and wishes to interrupt the packet, and in a destination, for example AODV, a malicious node Argues that it can send a fake route response (RREP) to the source node and provide the shortest route and new route to the destination node.

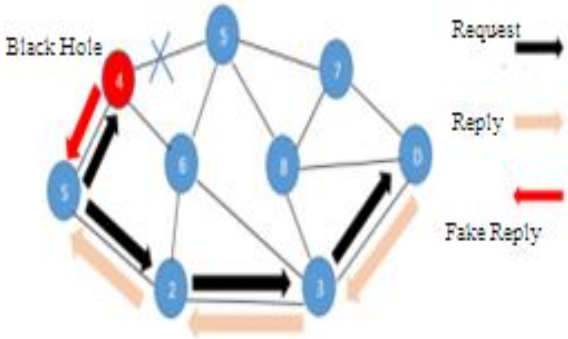


Fig 1: Black hole Attack [6]

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. Grey hole Attack

Gray Hole Attack is a kind of active attack that guides to the destruction of data packets. It is sometimes called a black hole attack.

C. Wormhole Attack

Wormhole attacks are also called tunneling attacks. It is one of the most serious attacks on MANET. In this attack, the collusion node creates a tunnel between the two nodes to send the packet, provides the shortest path to the destination, making it attractive to have complete control of the node [17]. Wormhole can drop packets by shorting the systematic flow of routing packets. Or you can send packets wisely to avoid detection.

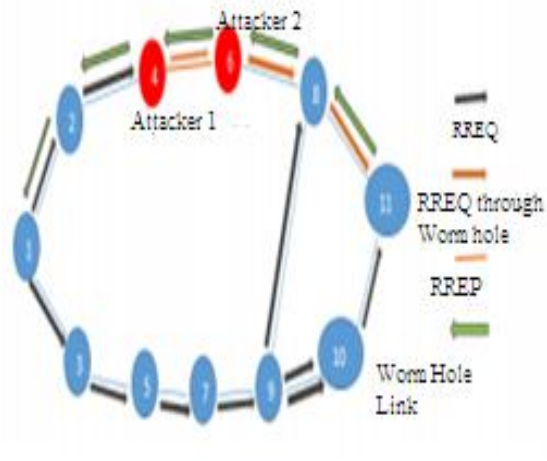


Fig 2: Wormhole Attack [6]

D. Sinkhole Attack

Sinkhole attack is a serious attack in mobile ad hoc networks. In sink hole attacks, the primary purpose is to attract all traffic from that intermediary node by telling them that the malicious or compromised node has the shortest part to the destination node [18].

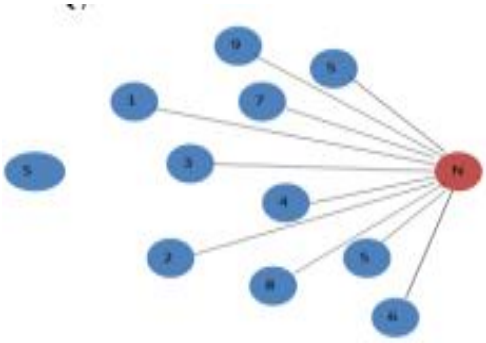


Fig 3: Sinkhole Attack [6]

IV. TRUST BASED SECURITY MECHANISM

This security instrument influences upon a trust management structure which has been shrouded in previously done works [17] for the recognition of malicious packet droppers which focus on the information plane security by carrying on genuinely at the time when the formation is going on and display the malicious behavior of the node at the state of information transmission by essentially dropping the parcels. The present paper centers upon the use of trust management structure in the plan of a novel security component for secure information transmission. In trust management scheme, for protecting the data plane during the occurrence of communication process, the malicious packet dropper are recognized and then this collected information is further used to create a secure path for communication establishments [19]. This is done by purging the malicious packet dropper nodes which was detected earlier communication process. Trust based security mechanism is defined in five phases as follow:

Let's consider an example there is a network where the each communication process consists of transmission of N packets and the existence of five phases are shown in section below:

Volume 5 Issue V, May 2017
ISSN: 2321-9653

A. Data Transmission phase

Firstly the source node will transfers the N packets and every concerned intermediate node will broadcast a link layer acknowledgement to its adjacent nodes [5]. The broadcasted acknowledgement comprises of a hash value which is unique for every transferred packet. The attached has value is pre evaluated and referred to create an acknowledgement report [20].

B. Report Request Phase

It is the second phase. In this phase the confirmation regarding the feedback of acknowledgement report corresponding to the every node which is concerned with the routing mechanism is generated [6].

C. Report Processing Phase

It is the phase which performs the evaluation of the received acknowledgement report in order to detect the nodes which are responsible to malicious packet dropper nodes and then these nodes are blacklisted or banned to perform communication.

D. Blacklist Propagation Phase

This phase is responsible to generate an alert message to each every node in the network regarding the blacklisted node [21]. Hence, the nodes became able to recognize the blacklisted node and did not allow that node to take participation in the route formation procedure.

E. Secure Route Establishment Phase

This phase inherits the information that is gathered by the blacklist propagation phase in order to discard the banned nodes from the future routes. This phase is also responsible for distribution of the pre evaluated has values to the concerned nodes by the destination node.

F. Trust Evaluation

The trust evaluation is the most important process included in the trust based security mechanism. The trust value is evaluated for a packet, a node or a route in the form of some threshold value [22].

The image shown in figure 4 depicts the process of trust evaluation.

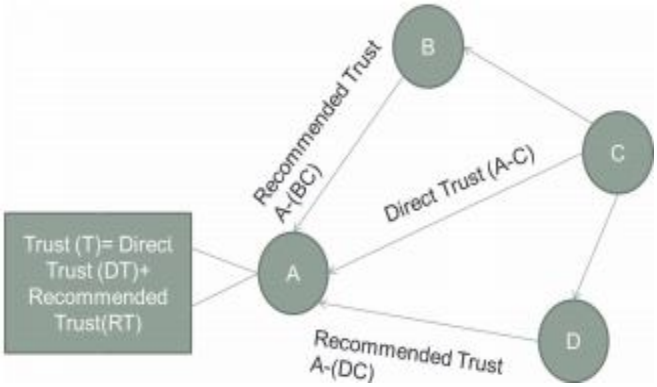


Figure 4 Trust Evaluation Process[15]

G. Direct Trust

Direct trust refers to the term or values which is evaluated for a node to another node. It is based on the process of communication with other node [23]. On the basis of this concept the actions of the network are categorized into two forms i.e. Positive events and Negative Events.

Positive events refer to the events or actions such as route error, route request, route reply or data flow. Whereas the events like flooding, deletion of routes, packet dropping falls into the category of negative events.

H. Recommended Trust

In this form of trust the node which provides reference corresponding to the particular node is known as recommender node [24].

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

The node, against which the reference is added in known as recommended node. In this the route data packets are responsible to obtain the recommendations.

V. FUZZY INTERFERENCE SYSTEM

Fuzzy system is a logical system which is in the form of many-valued logic. The truth table of these values lies between the range of 0 and 1, since Boolean logic supports the 0 and 1 only and considers the result either 0 or 1. It also supports the elements which are surrounded by the set may either have partial degree of membership means either element belongs to a set or not. These degrees are managed by any particular functions when applied with the linguistic variables. Fuzzy use linguistic variables in addition to quantitative variables in order to present vague concept. Membership function defines mapping of a membership value between 0 and 1 in the given input space. Universe of discourse is another term used for input space [13] [19].

Following figure 5 explains the working process of fuzzy system in brief. Firstly a crisp value is added to the fuzzy system as an input. Then Fuzzification process is applied to the crisp fuzzy values. Fuzzification is a process which converts the crisp values into fuzzy sets.

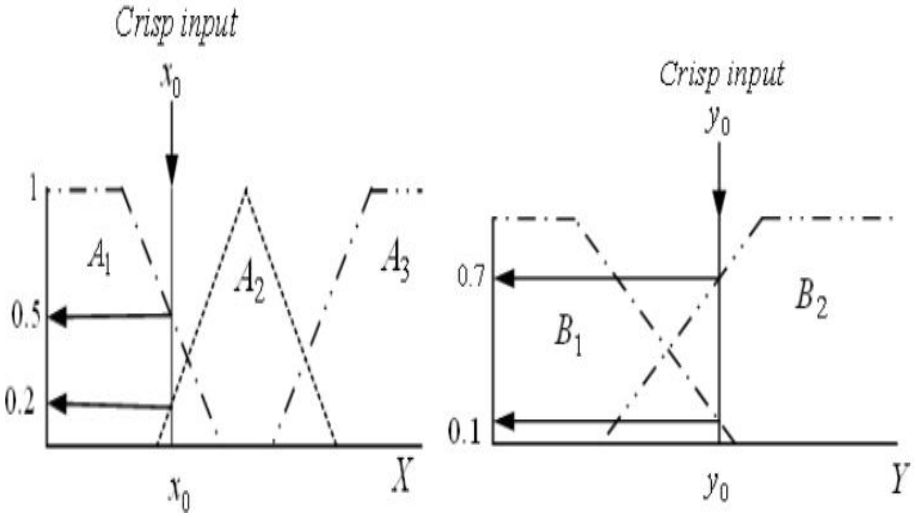


Figure5. Fuzzification [34]

Then defined rules are applied to the fuzzy input set driven by applying fuzzification. On the basis of rules an intelligent decision is taken and then the fuzzy sets are converted to the crisp values back by applying the Defuzzification.

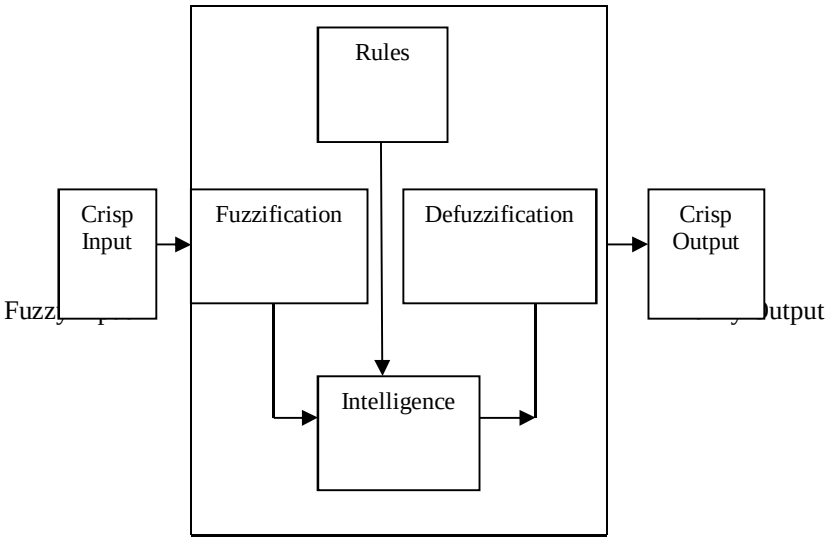


Figure6. Working of Fuzzy Logic Based System

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

VI. RELATED WORK

This section put a light on the few of the research works that were conducted in the direction of providing a trust based mechanism for securing the data plane in the ad hoc networks.

A. In 2016, Shuaishuai Tan et al [1] develops a security mechanism for data plane in the network which was based on fuzzy logics and graph theory. The objective behind implementing the fuzzy logics was to evaluate the path trust value on the basis of previous performance of the nodes and the graph theory was aimed to evaluate the node trust value. Along with this OLSR, filtering algorithm to sort out the problem of decaying the previous trust values from the trust table.

B. In 2015 Shirina Samreen et al [5] provides a solution to detect the malicious nodes in the MANETs which causes to the packet drooping in the network. The concept of malicious node detection was done by providing a trust based mechanism which uses the Dampster-Shafer Theory. The framework followed by this work in order to evaluate the trust value of the nodes is formulated as below:

$$\alpha(t+1) = \alpha(t) \times \tau_p(t) + p \quad (1)$$

$$\tau_p(t) = \gamma \times \frac{\alpha(t)}{\alpha(t+1)} \quad (2)$$

$$\beta(t+1) = \beta(t) \times \tau_q(t) + q \quad (3)$$

$$\tau_q(t) = \mu \times \frac{\beta(t)}{\beta(t+1)} \quad (4)$$

The trust evaluation of a node was based on the acknowledgement report that was generated by the source node.

C. In 2014 Z Wei et al [10] proposed a unified trust management mechanism on the basis of artificial intelligence technology. The proposed trust management mechanism was categorized in two parts i.e. trust from direct observations and another trust from indirect observations. The equation used for evaluating the trust value is composition of trust value corresponding to the direct observation and trust value from indirect observations.

$$T = \lambda T^s (1-\lambda) T^N \quad (5)$$

Formulation used for direct trust value is depicted by T^s and the corresponding formulation was as:

$$T^s = E_n[\theta] = \frac{\alpha_n}{\alpha_n + \beta_n} \quad (6)$$

And T^N depicts the indirect trust value and the derivation is as:

$$T^N = m_{j1}(H) \oplus m_{j2}(H) \oplus \ldots \oplus m_{jn}(H) \quad (7)$$

In case of direct trust state the Bayesian inference was implemented whereas in case of indirect trust observation Dampster- Shafer theory was applied to evaluate the trust value. These two mechanisms were combined in order to create more reliable trust mechanism for nodes in the MANETs.

D. In 2013, H Xia et al [11] presented a dynamic trust estimation model to calculate the trust factor of the nodes on the basis of their previous erformance and the future behavior by using the following equation.

$$TV_{ij}(t) = \frac{\sum_{k=1}^{n} f_k \times TV_{ij}(tk)}{\sum_{k=1}^{n} f_k} \quad (8)$$

The trust worthiness of the nodes was calculated by implementing the fuzzy based trust mechanism. The proposed model hybridized with the Source Routing algorithm in order to elect the shortest route for message delivery. The proposal was named as Trust based secure routing protocol i.e. TSR.

E. In 2011 Tameem Eissa et al [18] develops a FrAODV, a trust based mechanism which was created in order to secure the AODV routing algorithm. The basic idea was that the few of the parameters such as identity value and reputation value of the nodes were selected or considered to evaluate the routing path before handling he data over the nodes. The NS_2 and JADHOC

Volume 5 Issue V, May 2017
ISSN: 2321-9653

were used to simulate the proposed work.

The following table 1 provides the overview to the defined work in the section of related work.

Table1 Review to the related work

S. No.	Author(year)	Topic	Proposed Work
1	Shuaishuai Tan et al [1] (2016)	A Trust Management System for Securing Data Plane of Ad-Hoc Networks	Method:- Fuzzy Logics and Graph Theory Objective:- To evaluate the path trust value on the basis of previous performance of the nodes.
2	Shirina Samreen et al [5] (2015)	Trust based Data Plane Security Mechanism for a Mobile Ad hoc Network through Acknowledgement Reports	Method:- Dampster-Shafer Theory Objective:- The objective of this research work was to evaluate or detect the malicious or suspected node which causes the packet dropping while transmission of the data.
3	Wei et al [10](2014)	Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning	Method:- Bayesian Interference and Dampster- Shafer Theory Objectives: - To calculate the more accurate and reliable trust values of the observed nodes.
4	H Xia et al [11] (2013)	Trust prediction and trust-based source routing in mobile ad hoc networks	Method:- Fuzzy Interference System Objective:- To evaluate the trust value of the nodes on the basis of their previous performance and as well as future behavior too
5	Tameem Eissa et al [18] (2011)	Trust-Based Routing Mechanism in MANET: Design and Implementation	Method:- AODV algorithm Objective:- The aim of this study was to secure the AODV algorithm by introducing the friendship based framework.

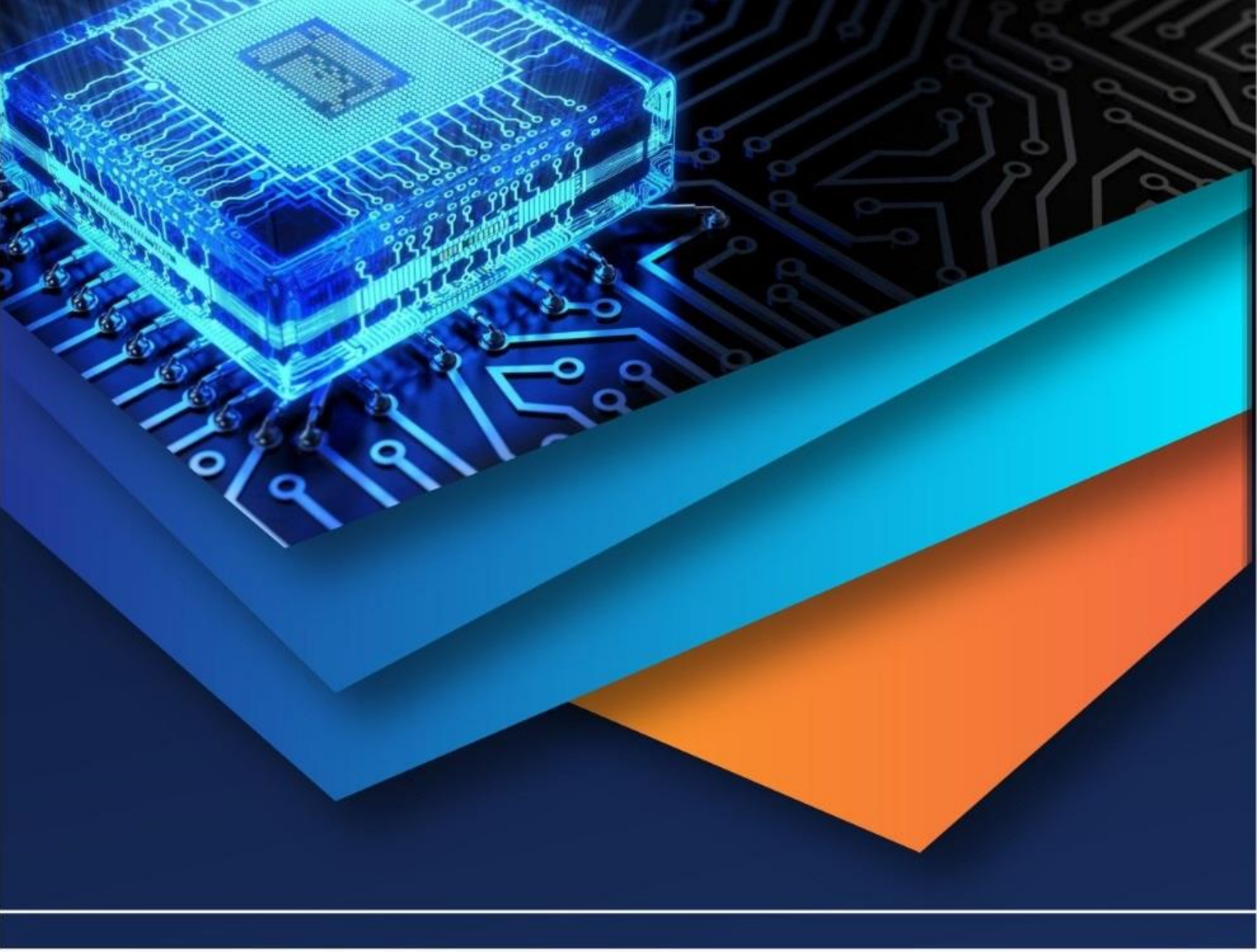
Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

VII. CONCLUSION

This segment of the paper provides a conclusion to the survey that is defined in the related work section of this paper. The emerged ad hoc network has a variety of applications like MANETs, VANETs and WSNs etc. because of its various features like dynamic topology and openness it faces various attacks to the data plane. No doubt lots of mechanism has been developed in last few years but after having an eye over the past work it can be compiled that the trust based mechanism can be considered for further enhancements by collaborating it with the advance mechanisms.

REFERENCES

[1] Shuaishuai Tan et al, "A Trust Management System for Securing Data Plane of Ad-Hoc Networks", IEEE, transactions on vehicular technology, vol. 65, no. 9, pp 7579- 7592, September 2016
[2] Sudha Dwivedi et al, "Review in Trust and Vehicle Scenario in VANET", IEEE, Future Generation Communication and Networking Vol. 9, No. 5, pp. 305-314, 2016
[3] Pooja Pilankar et al, "trust based security in manet", IJRET: International Journal of Research in Engineering and Technology, 2319-1163, Volume: 05 Issue: 02 , Pp 12-19, Feb 2016
[4] Shuaishuai Tan et al, "Trust based routing mechanism for securing OSLR-based MANET ", ELSEVIER, Adhoc Networks, March 2015
[5] Shirina Samreen et al, "Trust based Data Plane Security Mechanism for a Mobile Ad hoc Network through Acknowledgement Reports", International Journal of Computer Applications (0975 – 8887) Volume 129 – No.6, pp 6-13, November2015
[6] Bijender Bansa et al, "Attacks Finding and Prevention Techniques in MANET: A Survey", IEEE, Wired and Wireless Communications Vol.4, Issue 2, Pp 1-7, 2015
[7] Savitha. M et al, "A Study on Various Attacks in Wireless Ad hoc Sensor Network", International Journal of Computer Science and Mobile Computing, vol 3, issue 9, pp 231-243, September 2014
[8] Ranjitha.R et al, "Secure Wireless Ad-Hoc Sensor Network from Vampire Attack Using M-DSDV", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 5, pp 4081-4087, May 2014
[9] X. Anita, et al, "Fuzzy-Based Trust Prediction Model for Routing in WSNs", HINDAWI, Volume 2014 (2014), Pp 1-11, July 2014
[10] Z. Wei etal, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning," IEEE Trans. Veh. Technol., vol. 63, no. 9, pp. 4647–4658, Nov. 2014
[11] H. Xia, et al., "Trust prediction and trust-based source routing in mobile ad hoc networks," IEEE, Ad Hoc Netw., vol. 11, no. 7, pp. 2096–2114, Sep. 2013.
[12] Vanita Rani et al, "A Study of Ad-Hoc Network: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, vol 3, Issue 3, Pp 135-138, March 2013
[13] Ashish Kr. Shrivastava et al, "Study of Wormhole Attack in Mobile Ad-Hoc Network", International Journal of Computer Applications, vol 73, Issue 12, Pp 32-37, July 2013
[14] M. Marimuthu et al, "Enhanced OLSR for defence against DoS attack in ad hoc networks," J. Commun. Netw., vol. 15, no. 1, pp. 31–37, Feb. 2013.
[15] Kartheesan, L et al, "Trust Based Packet Forwarding Scheme for Data Security in Mobile Ad Hoc Networks", OSR Journal of Computer Engineering (IOSRJCE) 2278-0661 Volume 2, Issue 3, PP 40-48, July 2012
[16] D. Chasaki et al, "Attacks and defenses in the data plane of networks," IEEE Trans. Dependable Secure Comput., vol. 9, no. 6, pp. 798–810, Nov. 2012.
[17] P. F. Saverio, A. Detti, C. Pisa, and G. Bianchi, "A framework for packet droppers mitigation in OLSR wireless community networks," in Proc. IEEE ICC, pp. 1–6. 2011
[18] Tameem Eissa et al, "Trust-Based Routing Mechanism in MANET: Design and Implementation", SPRINGER, Mobile Netw Appl, Pp 1-12, June 2011
[19] Pushpita Chatterjee et al, "TRUST BASED CLUSTERING AND SECURE ROUTING SCHEME FOR MOBILE AD HOC NETWORKS", International Journal of Computer Networks & Communications (IJCNC), Vol.1, No.2, Pp 84-97, July 2009
[20] I. Aad, et al "Impact of denial of service attacks on ad hoc networks," IEEE/ACM Trans. Netw., vol. 16, no. 4, pp. 791–802, Aug. 2008.
[21] Bing Wu et al, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", SPRINGER, In Wireless network security, pp. 103-135. Springer US, 2007.
[22] Lidong Zhou et al, "Securing Ad Hoc Networks", IEEE, Pp 1-12, November 1999



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY