iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8142

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Security Issues in Mobile Adhoc Networks: Attacks and their Countermeasures

Kamna Sharma[1] , Harish Saini[2]
[1,2]*Computer Science and Engineering Department, GNI, Mullana, Haryana, India.*

Abstract: A Mobile ad hoc network (MANET) is a collection of mobile devices where each device participates in routing by forwarding data to other nodes. MANETs can be employed in various situations ranging from emergency operations and disaster relief to military service and task forces, so security is an essential component for protected communication between nodes. In this paper, we provided classification of security attacks in MANET into data, network, application and routing attacks. We further discussed and compared various countermeasures against these attacks.
Keywords: MANET, Attacks, Security, Detection, Routing

I. INTRODUCTION TO MANET

MANET is a collection of mobile nodes in which nodes communicate with each other through wireless links without relying on any existing infrastructure, centralized access points or base stations [1]. It is a flexible network and is self-configurable which allows network deployment quickly without the need of specified infrastructure.
These networks are useful in situations where either infrastructure is not available or installing the infrastructure is is very costly [2]. Application set of MANETs is very divergent. MANETs can be applied in military, voting systems, automated battlefields, rescue systems, mobile offices, electronic payments, and virtual classrooms, other emergency and disastrous situations. The characteristics of MANETs such as absence of trust relationship among nodes, power constraint lack of centralized authority and dynamic topology impose major security issues. The wireless channel is accessible by both legitimate users as well as intruders. It also lacks clear boundary between inside network and outside world.

II. SECURITY ISSUES IN MANETS

Security is the major concern in MANETS to maintain the security in wireless environment. Adversaries launch different type of attacks to disrupt the whole network by tampering the original messages. So, before we analyze diverse attack categories, we look at how attackers are classified on the basis of their nature and scope to destruct the system as follow [3]:

A. Active Attackers

These attackers are very harmful for the system because they generate the packets by modifying the actual content of the message and do not forward the acknowledged message.

B. Passive Attackers

These attackers spy on the wireless medium to gather useful information which may be moved to other attackers but do not engage in the communication process of the network.

C. Insider Attackers

These attackers are the legitimate users of the network and have the concrete knowledge of the network. They are very dangerous as compared to other attackers because it's simple for them to fire attacks against the network.

D. Outsider Attackers

These are invaders who have goal to exploit the network but they generate lesser problems as compared to the insider attackers.

E. Rational Attackers

These attackers launch attacks for the purpose of getting personal benefits.

F. Local Attackers

These attackers fire an attack which is confined to a particular area.

III. CLASSIFICATION OF ATTACKS IN MANETS

There are diverse attacks that harm the security of the MANETs by disturbing the whole network and the confidentiality of vehicles. The attacks that have drastic effect on the services of the system are discussed below:

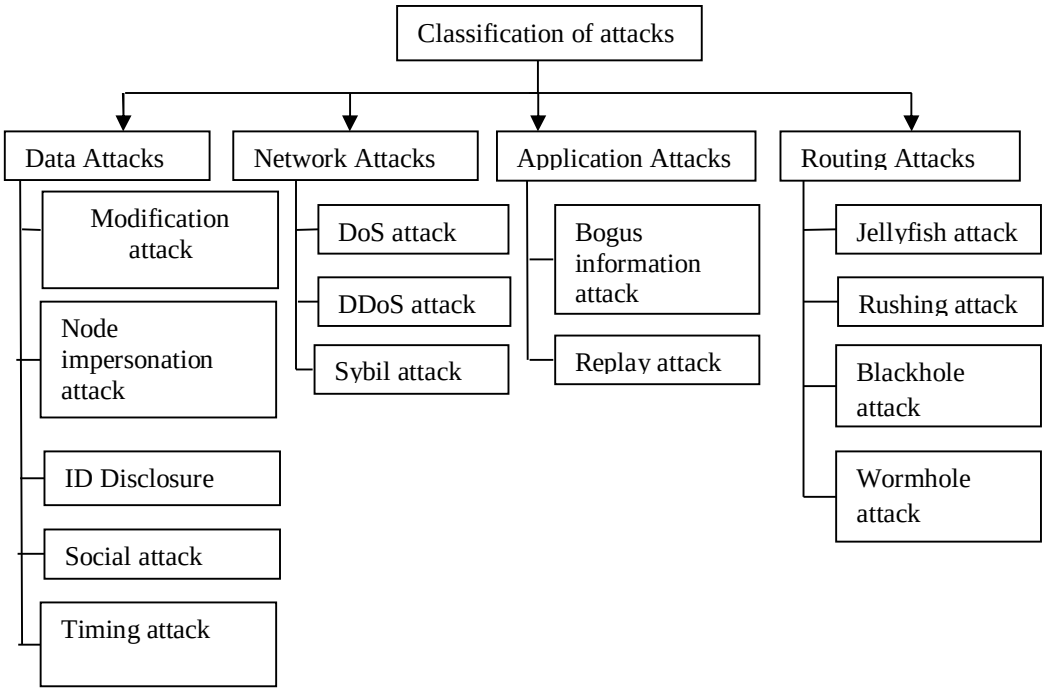


Figure 1: Classification of attacks

A. Data Attacks

These are the attacks in which attacker tampers the data and forwards the fake data in the network. Following attacks come under the category of data attacks:

1) *Modification Attack:* This is the attack in which an attacker modifies the actual content of the message and forwards it in the network. Thus creates confusion in the whole network.
2) *Node Impersonation Attack:* This is the network attack in which attacker modifies the original content of the message and forwards it in the network by claiming that message has been originated from the authorised user. Greedy algorithm is used to detect and isolate the node impersonation attack.
3) *ID Disclosure:* This is the network attack in which attacker tracks the location of destination node by disclosing the identity of nodes in the network. Observer looks at the destination node and relay the virus to the neighbours of the destination node so that ID and the location of the destination node can be taken.
4) *Social Attack:* The main goal of this attack is to puzzle and fascinate the vehicle by sending correct and incorrect messages so that driver gets upset [4]. It indirectly creates the problem in the network so that authenticated user exhibits angry behavior which is the main objective of the attacker.
5) *Timing Attack [14]:* Timing attack is very crucial for safety applications. This is the attack in which an adversary adds some time slot in the authentic message but do not modify the content of the message and thus create a delay in the authentic message [5]. With this the collision occurs, thus it creates a major problem for the drivers because drivers do not receive the information on time.

B. Network Attacks

These are the attacks in which attackers directly affect the vehicles by disturbing the whole network. There are the following attacks that come under network attacks are:

1) *Denial of Service (DoS) Attack:* DOS is one of the dangerous attacks in VANETs. In DOS attack, attackers use the vehicle resources and create a troublesome situation by jamming the communication channel so that authenticated users cannot be able to access the network services. For e.g. Jamming attack is the DOS attack
2) *Distributed Denial of Service (DDoS) attack:* In DDOS attack, attacker use the multiple computers to launch attack and uses the different locations and time slots to send messages to other vehicles. The main goal of the DDOS attack is to halt the network.
3) *Sybil Attack:* Sybil attack allows an attacker to create multiple false identities known as Sybil nodes which will behave as a normal node [6]. It provides false belief to other vehicles by sending erroneous messages such as traffic jam etc and each message contains the formulated id. The main objective of an attacker is to disturb the whole network for their personal benefits.

C. Application Attacks

These are the attacks in which attacker modifies the content of the message for taking personal advantage. The attacks described below are the application attacks:

1) *Bogus Information Attack:* In Bogus information attack, the adversary may be outsider or insider [7]. The main objective of an adversary for launching this attack is to send erroneous or bogus information in the network to create disturbance and for his personal benefits.
2) *Replay Attack:* In replay attack, the attacker takes an advantage by replaying past messages in order to confuse the authorities and creating a jam among vehicles.

D. Routing Attacks

These are the attacks in which attacker spoofs the routing information by launching diverse attacks on routers which are described below:

1) *Jellyfish Attack:* In Jellyfish attack, attacker intends to minimise throughput of network by reordering the packet sequence, dropping or delaying the packets [8]. In this attack, attacker node became a part of network after getting access of it. It is similar to blackhole attack with dissimilarity in terms of dropping the packets, blackhole attack drops all the packets but jellyfish (JF) attacker drops periodically. There are three types of Jellyfish attack as shown in Fig 2.

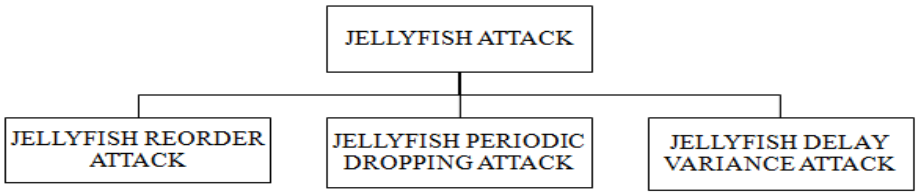


Figure 2: Types of jellyfish attack

2) *Rushing Attack:* In this attack, every node before broadcasting the data, first established an authentic way to the destination node using a routing protocol such as AODV, DSR etc. The attacker set a fast transmission path by exploiting the duplicate suppression mechanism to forward the packets. With this process the destination node accepting the packets those are propagated faster than the multi-hop normal route and start dropping the original packets. This forms the rushing attack.
3) *Black Hole Attack:* In this attack, an attacker introduces a malicious node in the network which attracts all other nodes and pretending as the original one [9]. When all other nodes make a false belief on the malicious node and start sending packets through the malicious node then it selectively drop the packets.
4) *Wormhole Attack:* This is the attack in which attacker joins the two faraway parts of ad-hoc network using an additional communication channel as tunnel. The tunnel records the ongoing communication at one network position and transmits the recorded communication at other network position. This process is also known as tunnelling [6]. To launch this attack, attacker introduces two malicious nodes which are assumed as neighbour nodes that help to transfer the data using tunnel. The malicious nodes attract the other nodes by advertising the shortest path among them so that they can be able to transfer the packets from

one network to another network. The path introduced to transfer the packets is harder to predict because it is not a part of real network.

IV. COUNTERMEASURE AGAINST ATTACKS

Security is an important part of all kinds of networks including mobile ad hoc networks and the security related issues for wireless networks are more difficult than the ones for wired networks and this is because of the rapidly changing unpredictable topology formation by mobile nodes and like battery constraint and bandwidth constraint [10]. Nodes in mobile ad hoc networks are power constrained and there is no alternate power source. Adversary can send huge traffic to the victim or target node and force the target node to exhaust its battery while handling these packets. This results in denial of service attack because node is now exhausted and cannot participate in other services of the network. Another security issue is the presence of selfish nodes which do not cooperate to routing or forwarding the packet to reserve their battery. When majority of nodes behave in a selfish manner, the whole system may collapse [11].

Many countermeasures have been proposed in the literature to thwart security attacks described in Section 3 to protect MANET environment against malicious and selfish nodes. These solutions constitute standalone protocols or incorporation of security mechanism into existing routing protocols namely AODV, DSR, OLSR etc. These are divided into preventive and reactive mechanisms. The conventional mechanisms such as authentication, digital signatures, MAC, HMAC and encryption constitute a layer of preventive mechanism. Reactive mechanisms including intrusion detection systems (IDS), trust management systems and reputation systems constitute a second layer of defense against security attacks.

A. Cryptography Based Solutions

Many of the aforementioned attacks such as alteration, impersonation, replay etc poisoning could be prevented by using strong authentication and encryption mechanisms relying on asymmetric, symmetric and hybrid cryptography.

Nikam and Raut [12] proposed a new technique for intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) with Elliptic Curve Algorithm (ECC) for MANETs. The proposed technique can withstand shortcomings of Watchdog mechanism [13] including false misbehaviour, receiver collision and limited transmission power. Elliptic curve Digital Signature Algorithm (ECDSA) is used to thwart the attackers from forging acknowledge packets. It comprised of Acknowledge, Secure Acknowledge, Misbehavior Report Authentication and lightweight ECDSA. The results obtained proved that it outperforms existing schemes in terms of throughput and end to end delay.

Sharma et al. [14] proposed a cryptographic technique based on identity based encryption (IBE) and visual cryptography for military surveillance. IBE is used by base station for initial setup, thereafter RSA algorithm is used for encryption and decryption. The simulation is carried in Matlab and C++ using open-ssl cryptograohic library. Ravilla and Putta [15] proposed secure ZRP routing protocol using HMAC-SHA512 and a keyed-HMAC-SHA512 for providing data integrity and authentication. It employs a secret key along with the hash function to send data from source to destination securely.

B. Intrusion Detection

The cryptographic mechanisms thwart against known attacks and consume much battery power and other resources of mobile nodes. Intrusion detection system (IDS) is introduced to detect malicious and selfish nodes in a network. An IDS comprise of mechanisms and methods to detect suspicious activities and generate alert about intrusions.

Wazid et al. [16] proposed Cluster Based Intrusion Detection and Prevention Technique (CBIDPT) and Super Cluster Based Intrusion Detection and Prevention Technique (SCBIDPT) for detection and prevention of JF reorder attack. CBIDPT performs well in case of intermediate node acting maliciously and fails when cluster head behaves maliciously whereas SCBIDPT performs well in presence of malicious cluster head also. Cluster head compares all sequence numbers of packets stored in its buffer to the sequence numbers of packets stored in buffer of all intermediate nodes to detect misbehaving node.

Poongodi and Bose [17] proposed novel IDS using the trust evaluation metrics for the detection of the flooding DDoS attacks. The proposed TEB-SOT-FCN IDS combines the existing Firecol-based security procedures [18] with Dynamic Growing Self-Organizing Tree Algorithm [19] in the trust evaluation-based environment. The simulation results show that the proposed IDS performs better in terms of performance metrics such as packet data ratio, throughput, average delay and energy consumption.

Gautam et al. [20] proposed a fuzzy based IDS to mitigate RREQ flooding attack in MANET environment and reduce the loss of throughput. The simulations were carried on NS-2. RREQ flooding attack drops packet delivery ratio to 15 with single malicious node and fuzzy based detection algorithm increases packet delivery ratio to 71.66 as compared to 72.16 in normal AODV without attack. Normalized routing load increased from 0.48 to 4.22 with attack and proposed scheme reduces it to 1.28.

C. Trust Management and Reputation-Based Systems

Many research efforts have been made to address the security issues for MANETs using trust management and reputation-based systems. Watchdog and Pathrater [13] scheme which is an extension for DSR routing protocol, that introduces two related techniques to detect and mitigate the impact of nodes that do not forward packets. The watchdog extension monitors and verifies that the next node in the path forwards packets properly, otherwise misbehavior will be recognized. The path-rater evaluates the results of the watchdog and selects the most reliable path for packet delivery. CONFIDANT [21] is a reputation-based scheme which is capable of detecting selfish nodes by observing routing and packet forwarding behavior of other nodes through their own experience, overhearing neighborhood traffic and from the trusted second hand observations from their neighbors. COllaborative REputation CORE [22] is a reputation-based system that deals with network level selfishness. Each node keeps track of other nodes' reputation computed on the basis of self monitoring and information gathered from other nodes. A punishment mechanism is used to isolate misbehaving nodes by ignoring their requests.

Ravilla and Putta further proposed a trust based secure ZRP combining HMAC-SHA512 and trust based routing [15]. The trust value of a node is increased whenever it transmits a packet and decreased otherwise. The simulation is carried on NS2 with varying number of nodes and zone radius. Azer et al proposed a Functional REPutation system for Ad hoc Networks (FREPAN) [23] to mitigate selfish and malicious nodes. It comprises of four modules: observer, modeler, hybrid dissemination and decision making module. The observer module monitors the network and aggregates direct and indirect information about each node from neighbors by use of the watchdog component [13] in the promiscuous mode. The modeller module combines all the information gathered into a meaningful reputation values whereas dissemination module propagates these reputation values. The decision making module penalizes node exhibiting malicious behaviour.

Anjugam and Muthupriya [24] proposed a light-weight Direct Trust-based Detection (DTD) algorithm and Monitor, Detect, Rehabilitate (MrDR) technique to detect a JellyFish node from an innovative transmission route. They analyzed the effects of three JF (Jelly-Fish) attack variants: JF-reorder, JF-delay and JF-drop over TCP-SACK. In DTD algorithm, trust value was estimated by each node to determine whether its neighboring node is JF-attacker or not over a time period. The Monitor, Detect, Rehabilitate (MrDR) technique, is applied as an enhancement to further detect and eliminate jellyfish attack.

Table 1: Comparison of detection and preventive schemes against routing attacks in MANET

Scheme	Based on	Attacks	Routing protocol used	Merits	Demerits
EAACK with ECC [12]	Elliptic Curve Crptography	Packet dropping attacks	AODV	The results demonstrated constructive performances against Watchdog, TWOACK, AACK and EAACK in the cases of receiver collision and limited transmission power false misbehavior report and End to End delay.	This algorithm does not work well with multipath routing.
IBC and Visual cryptograpghy [15]	Identity based encryption, RSA	Data attacks	-	The implementation supports data and image transfer from mobile nodes to base station and fro in parallel and for this the pthread library plays the key role. Regeneration of public-private keys after certain threshold period makes system more secure from attacks.	Further efforts are being made to reduce the setup time of the base station and improving the time complexity of the above mentioned Algorithm.
CBIDPT and SCBIDPT [16]	Intrusion Detection system	Jellyfish reordering attack	AODV	Detects and prevents JF reorder attack in both environments i.e. intra-cluster and inter-cluster. Th goodput of network has improved to 1022.07 kbps from 0 kbps in	These schemes introduce delay in the network.

				presence of JF attack.	
TEB-SOT-FCN [17]	Intrusion Detection system	DDoS Attacks	AODV	IDS with trust-based evaluation has minimum average latency, maximum throughput and better detection rate (95.8%) in comparison to Firecol and Firecol-based DGSOT algorithms.	The trust evaluation is designed for homogeneous networks only.
Fuzzy based IDS [20]	Intrusion Detection system	Flooding attack	AODV	Fuzzy based IDS increases packet delivery ratio from 15 to 71.66 with single malicious node.	Considered only number of route request packets and residual energy as fuzzy parameters.
Trust based ZRP [15]	HMAC, SHA-512, Trust	DoS Attacks	ZRP	Trust-Based system isolates malicious nodes to increase throughput and packet delivery fraction.	The tolerable limit of malicious node is less than 30%. The end to end delay for the trust based system increases
FREPAN [23]	Reputation based	Jellyfish attack	AODV	It avoids false accusation for benign nodes. It depends on promiscuous information collected indirectly to minimize network's traffic overhead.	There is significant average end to end delay. The nodes have to work in promiscuous mode.
Lightweight DTD and MrDR [24]	Trust management based	Jellyfish attack	AODV	This schemes achieves high throughput as compared to DTD algorithm. It identifies and removes JF nodes dynamically.	It may result in false JF-attacker detections due to improper overhearing of data packets in promiscuous mode

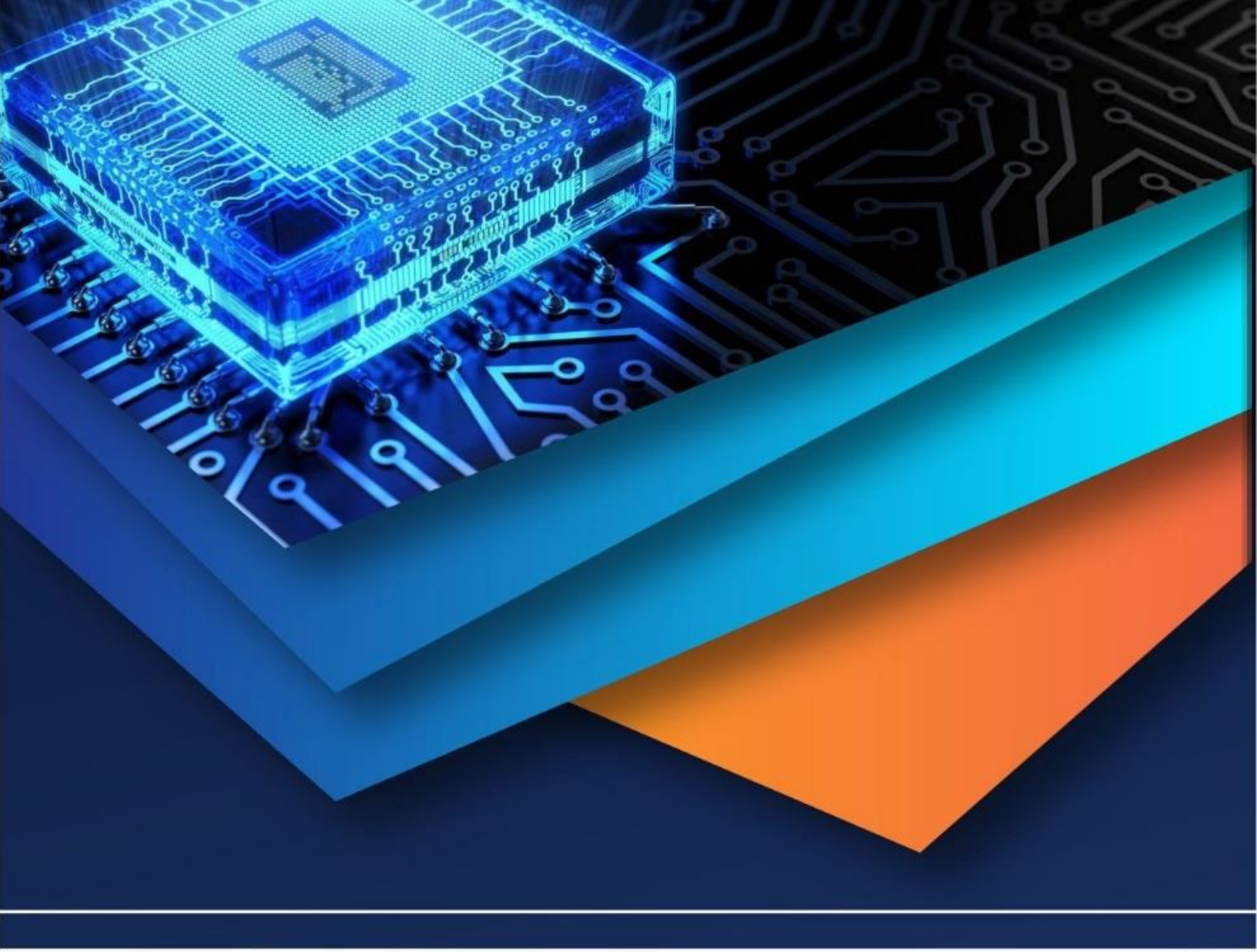
V. CONCLUSION AND FUTURE SCOPE

In this paper, we reviewed the current state-of-art of security issues in MANET. Security can be easily jeopardized if proper countermeasures against attacks are not taken. Because of easy deployment and absence of predefined infrastructure, MANET found applications in military services, task forces and emergency rescue operations. Security is very critical in such scenarios. As discussed above, the solutions work with specific attack and are still vulnerable to unexpected attacks. Therefore, researchers should design secure protocols that prevents all possible attacks, detects unexpected attacks and reacts to exclude malicious nodes from the established route to make MANET a secure and reliable network.

REFERENCES

[1] Nguyen H.L and Nguyen U.T, "A study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Networks, vol. 6, no. 1, pp. 32-46, 2008.
[2] Bhatia, T., and Verma, A.K. (2015). "QoS Comparison of MANET Routing Protocols", International Journal of Computer Network and Information Security, 9, pp. 64-73.
[3] S. S. Tangade and S. S. Manvi, "A Survey on Attacks, Security and Trust Management Solutions in VANETs," in 2013 Fourth International Conference on Computing, Communications and Network Technologies, Tiruchengode, 2013.
[4] A. Sumra et al. "Classes of attacks in VANET In Electronics,, (pp. 1-5). IEEE." in 2011 Saudi International in Electronics, Communications and Photonic Conference (SIECPC), Riyadh, 2011.
[5] I. A. Sumra, J. L. Ab Manan and H. Hasbullah, " Timing attack in vehicular network," in World Scientific and Engineering Academy and Society (WSEAS) in Proceedings of the 15th WSEAS International Conference on Computers, Corfu Island, 2011.

[6] Goyal, S., Bhatia, T., Verma, A.K. (2015). "Wormhole and Sybil Attack in WSN: A Review", INDIACOM 2015:09th INDIACOM, 2nd IEEE International Conference on Computing for Sustainable Global Development, pp. 1463-1468.
[7] V. H. La and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: a survey," International journal on AdHoc networking systems (IJANS), vol. 4, no. 2, pp. 1-20, 2014.
[8] H.P.Chatar and S.Waghmare, "Vehicular Ad Hoc Networks (VANETS): Attacks and Challenges: A Survey," International Journal of Electronics, Electrical and Compuational System (IJEECS), vol. 4, no. 4, pp. 60-64, 2015
[9] Bhatia, T., and Verma, A.K. (2013). "Performance Evaluation of AODV under Blackhole Attack", International Journal of Computer Network and Information Security, 5 (2), pp 35-44.
[10] Bhatia, T., and Verma, A.K. (2013). "Security Issues in Manet: A Survey on Attacks and Defense Mechanisms", International Journal of Advanced Research in Computer Science and Software Engineering, 3 (6), pp. 1382-1394.
[11] Yang H., Luo H., Ye F., Lu S., and Zhang L., "Security in mobile ad hoc networks: challenges and solutions." Wireless Communications, IEEE, vol. 11, no. 1, pp. 38-47, 2004.
[12] Nikam, P. D., & Raut, V. (2015). Improved MANET Security Using Elliptic Curve Cryptography and EAACK. In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on (pp. 1125-1129). IEEE.
[13] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265). ACM
[14] Sharma, R. K., Kishore, N., & Das, P. (2014). Secure and efficient application of MANET using Identity Based cryptography combined with Visual cryptography technique. International Journal of Engineering And Computer Science, 3(2), 3933-3937.
[15] Ravilla, D., & Putta, C. S. R. (2015). Enhancing the Security of MANETs Using Hash Algorithms. Procedia Computer Science, 54, 196-206.
[16] Wazid, M., A. Katal, and R. H. Goudar, "Cluster and super cluster based intrusion detection and prevention techniques for JellyFish Reorder Attack."Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on. IEEE, 2012.
[17] Poongodi, M., & Bose, S. (2015). A Novel Intrusion Detection System Based on Trust Evaluation to Defend Against DDoS Attack in MANET. Arabian Journal for Science & Engineering (Springer Science & Business Media BV), 40(12).
[18] François, J.; Aib, I.; Boutaba, R.: FireCol: a collaborative protection network for the detection of flooding DDoS attacks. IEEE/ACM Trans. Netw. 20(6), 1828–1841 (2012)
[19] Poongodi, M.; Bose, S.: A firegroup mechanism to provide intrusion detection and prevention system against DDoS attack in collaborative clustered networks. Int. J. Inf. Secur. Priv. 8(2), 1– 15 (2014).
[20] Gautam, S., Moudgil, S., and Bhatia, T. (2016). "Fuzzy Logic Based Intrusion Detection Scheme against DoS Attack in MANET", International Journal of Research in IT, Management and Engineering, vol. 6, pp. 21-27.
[21] S. Buchegger, J.Y. Le Boudec. Performance Analysis of the CONFIDANT Protocol. In proceedings of MobiHoc, ACM Press, 2002. pp. 226–236.
[22] P. Michiardi, R. Molva. Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. IFIP - Communication and Multimedia Security Conference 2002, pp. 107-121.
[23] Azer, M. A., & Saad, N. G. E. D. (2015). Prevention of Multiple Coordinated Jellyfish Attacks in Mobile Ad Hoc Networks. International Journal of Computer Applications, 120(20).
[24] Anjugam, S., & Muthupriya, V. Direct Trust-Based Detection and Recovery Process of Jellyfish Attack in Manet. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) Volume 22 Issue 2 – MAY 2016, pp. 32-38.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY