International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 48 – 58

A Survey on MANETs: Entrusted Security Challenges

Iram Nausheen*[1], Dr.Akhilesh Upadhyay[2]

[1,2]*Department of Electronics & Communication,SAGE University,Indore,India*
[1*]*iramnausheen@gmail.com*,[2]*akhileshupadhyay@gmail.com*

Abstract

An essential and challenging part of all future network and wireless communication system is Mobile Ad hoc Network (MANET) observed in applications e.g. cloud, reconfigurable network, Internet-of-Things (IoT), inter-domain routing, healthcare, wildlife, etc. However, the security problems in MANET is yet to be controlled fully irrespective of many security ways and solution. To stand a MANET system with upcoming technologies it is required that their routing system should offer potential against all threats as well as they should also offer a further flexibility to adapt the security schemes based on changing demand of the environment, where the mobile nodes are operating. There are many security attack measures need to be rectified by communicating between the protocol layers to contribute towards security system in MANET. Therefore, this paper offers review to the current situation of security system using conventional to explore its research gap.

Keywords: *Mobile Ad-hoc Network, Security attacks, Routing protocols.*

1. Introduction

Mobile Ad hoc Network (MANET) has been a constant research area among community from the past decade due to its feature of cost effectiveness associated with communication [1] [2]. Due to the quality of lack of infrastructure, MANET is familiar to provide speedy communication performance over its unorganized environmental condition. Irrespective of various applications of MANET [3] [4], they have many disadvantages too. The important reason for various challenges associated with MANET is its unorganized and decentralized architecture and its dynamic nature of topology causing random changes over the routing information over routing paths [5].

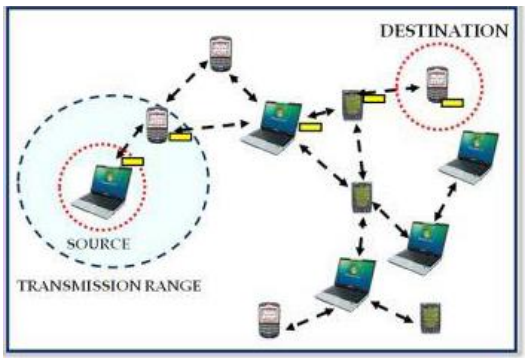

Fig.1 .Mobile Ad-hoc Network (Manet) [6]

The prominent characteristics for causes of the security challenges in MANET are

1. Dynamic Topologies
2. Fair chances of presence of lethal threats within a network,
3. No centralized management, limited physical security.

4. Bandwidth-constrained, variable capacity.
5. Energy Constraint operation etc [7].

Approaches towards security in MANET can be basically of two types. The first type is related to securing routing scheme [8] and second type is related to data security scheme [9]. Usage of routing protocols are the common way to deal with security problems where reactive routing protocols are used for threat identification and faster response time while table-driven routing schemes are mainly aimed on opposing conflict from intruders. The usage of key-agreement protocols are not much supported in MANET because of the infrastructure less nature. Moreover, it is quite improbable to establish a trust-based factor within the mobile nodes.

As the quickly moving and changing of nodes in MANETs, designing and establishing proper communication is a challenge and networking protocols for these networks is a tough process to take. In communication process designing of the routing protocols is a key aspect which are used to set up and maintain multi-hop paths to allow the data to communicate among nodes. Sufficient investigations has been done in a communication network area to develop multi-hop routing protocols. Among these protocols many of them such as the DSDV [10], Dynamic Source Routing protocol (DSR) [11], Ad-hoc on-Demand Distance Vector routing protocol (AODV) [12], Temporally Ordered Routing Protocol (TORA) [13], and others setup and maintain routes in the best way. It might be significant for a certain category of MANET applications, but it may happen to be insufficient for the support of more upcoming applications such as streaming of multimedia audio and video. Such kind of applications require the network to provide assured Quality of Service (QoS). Active research is carried by many researchers over the areas of QoS support in MANETs, and many QoS routing protocols have been already proposed in such conditions. Few of these protocols help in providing QoS support for the given path's link availability. As the link availability predictions can improves the service of routing protocols in such scenarios. Ad-hoc routing strategies can be categorized as: 1) Table-driven or proactive routing strategy , 2) This is a source-initiated and is called as demand-driven or reactive strategy, 3) Another one is a hybrid approach that uses many of the properties from both the proactive and reactive strategies. Figure 2 depicts this classification.

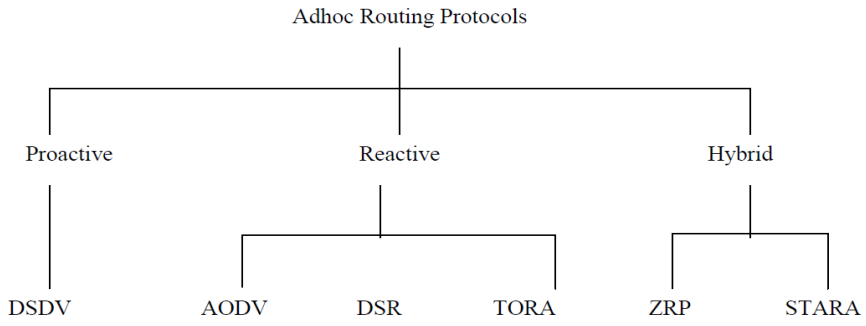

Fig.2 . Categorization of Ad-hoc Routing protocols

Moreover, such forms of wireless communication channel are highly prone to intrusion owing to different routing-based attacks [14]. Such forms of attacks also lead to

secondary intrusion e.g. sensitive data leakage, eavesdropping passively, tampering with confidential data, impersonation, denial-of-service, etc. Two types of attack strategies:

i) Attacks towards outbound data
ii) Attacks towards core operations of mobile nodes.

However, basically the standard classification is for only two types of attacks i.e. internal and external attacks [15]. Further, it has been seen that external attack is further divided into active and passive attack. The direct actions performed by the intruder node give rise to the active attack while eavesdropping operation results in passive attack.

It is being observed by researchers that internal attackers are the most challenging form of intrusion in MANET, which was found to be difficult to identify and resist as well. Such form of attack could perform unauthorized broadcasting of forged information of routing to neighboring nodes in a way such that one regular node is totally bounded of an attacker. Such captivated regular node is termed as compromised mobile node or internal attacker. Such node bears the capability of generating unauthorized signature with an aid of private keys. However, the presence of dynamic topology will further worsen the case. Moreover, passive attack is about obtaining sensitive information in stealth mode from the routing operation. The purpose of passive attack is to reveal the confidential information to the attacker that could let the conflict control the sensitive information of the mobile nodes.

Even though there has been various dedicated approaches toward securing MANET applications, but still the security problems are at large. This paper contribute to brief out the existing security solution in MANET as well as to promote the usage of other approaches. The aim is to take out the research gap. Organization of the paper in sections as below: Section-2 discusses MANET challenges and Issues, Section-3 discusses about important significance of MANET security followed by discussion of problems associated with existing security solution, in Section-4 various security entrusted approaches in MANET are explored, Section-5 shows the existing different MANET security solutions, in Section-6 research gap is presented and in Section-7 offers conclusive remarks of the review paper.

2. MANETs Entrusted Challenges and Issues

2.1 Obstructions/Challenges

The major challenges encountered by the MANETs can be commonly classified as:

a) In adaptive and modifying wireless networks, elements such as Mobile devices, ad-hoc routers and embedded sensors in the existing various protocol frameworks.

b) Provision of end-to-end service formulations that could help application development. These challenges are issued in a view of broad range of elements such as cellular data services, Wi-Fi hot-spots, Info stations, mobile peer-to peer networking, Ad-hoc mesh networks such as on the fly networks, broadband access, vehicular networks, sensor networks and there use in universal systems. These wireless applications may lead to a various combo of service requirements for the future is as briefed here[16]:

    1. Various nodes naming and addressing flexibility.
    2. For End-users and network devices, a relevant mobility support while their dynamic relocation.
    3. Provision of information on geographic positioning led location services.
    4. For distributed control of network topology its self-organization.

5. Requirements for security and privacy in mobile nodes and wireless channels of open nature.
6. Remote monitoring and control requires decentralization management.
7. Optimized performance of protocols can be done by cross layer framework.
8. Features such as aggregation, content routing and in-network processing in Sensor network.
9. For networks Cognitive radio support is required along with adaptation of physical layer
10. Efficient resources sharing should be encouraged though monetary policies.

2.2 Active Issues

Notable issues for MANETs are explained as below:

1. It is self configured and Autonomous in nature as there is no consolidated structure i.e. infrastructure less, available to manage the operation of the different mobile nodes, i.e. self operated and discontinuity of the changing links may occur due to self configuring nature.

2. By having dynamic topology because of the nature of Nodes which are mobile in nature and can be dynamically connected in an arbitrary manner. As a result the links of the network vary with time and are due to the close vicinity of one node to another node.

3. As Device discovery is dependent upon the recognition of appropriately newly found nodes and informing about their existence. This proposes a need to make automatic optimized route selection for dynamic updating.

4. Because of the lower capacity of Wireless links than the wired links. It has limited Bandwidth of radio band to offer data rates. It becomes an issue in Mobile Ad-hoc Networks as the throughput of wireless communications which has been realized after taking account the effects of multiple access, fading, noise, and interference conditions, etc.

5. Mobile nodes depend upon the battery power, and maintenance for a longer duration of which is a scarce resource because every node is light weighted so with small battery backup and small memory size. As this limits the storage capacity and power severely.

6. In the presence of a large number of nodes whether the network is scalable or able to give an acceptable level of service or not.

7. Any node in a network is free to enter or leave that is the mobility can be in shared media wireless network. So any malicious activity by a node cannot be tracked completely because it may be accessible by malicious attackers and authorized network users which limits the physical security.

8. Poor Transmission Quality arises in wireless communication by several sources of error caused by inner nodes as well as outer nodes that ultimately weakens the received signal.

9. Maintaining topology is a major issue because updating information of dynamic nodes is related to change in links every time the node changes or switches.

3. Significance of MANET Security

ISSN: 2233-7857 IJFGCN

Like other wireless networks, Ad-hoc networks requires security policies and implementation in realization of security goals. These may be spotted as below:

- Authentication
- Integrity
- Confidentiality
- Non-repudiation
- Availability
- Data Freshness

Most of the goals have some commonality with other networks except data freshness. As Ad-hoc networks has no centralized control. The decentralized control lead to poor synchronization in the networks to mislead the part of nodes as malicious or selfish nodes. This is why data freshness in Ad hoc networks has considered in security goals of MANET [17] application, better redundancy management, and supportability of time-bound emergency services.

As MANET is easily exposed to exponential larger network which is affected by trillions of malwares due to usage of internet and this becomes the challenging part to offer powerful security protocol. Another challenging aspect is to develop an efficient routing scheme that offers a good balance between the security demands and communication demands too. It is because if MANET is used with application in IoT systems, then there are inclusions of different heterogeneous routing schemes to affect the communication process too. Therefore, MANET security is definitely not an easy way to achieve [18].

The significant problems associated with existing literature is that it shows different forms of categorization of intrusions in MANET. According to Nadeem and Howarth [19], the attacks in MANET are normally of two type viz. passive attack (e.g. location disclosure, eavesdropping, and traffic analysis) and active attack (routing and malicious packet dropping). Further, the authors also said that enough vulnerability is within routing attacks only (e.g. blackhole attack, rushing attack, grey hole attack, Sybil attack, and sleep deprivation attack). Another recent work of in [20] discussed that flooding attack is the most deadly among all and hence the authors have presented classification of flooding attack as two types viz. continuous attack (ASRRF[20],NASRRF[20]) and selective attack (ASDF [20], NASDF [20]).Fig.3 highlights the standard taxonomies of attacks.

Depending upon the various layer based protocols which are different at every layer. Active attacks on different layers are very much different e.g. Signal jamming occurs in physical layer while disruption of MAC layer can be seen as active attack mode for link layer. Wormhole, overflow of routing, blackhole, wormhole, Byzantine, rushing, cache poisoning, etc are attacks on network layer. Session hijacking is witnessed in Transport layer. As the active model of attacks at application layer in MANET as mode of active attacks is from reputation, Trojans, malwares, virus, etc. these are reported in MANET as compared to other layers.

All these layers has common passive attack mode e.g. traffic analysis, eavesdropping, and monitoring, while network layer exclusively uses location disclosure attack as passive attack mode. However, at present, various mechanism and security-based solution is already offered to solve such security problem. For an example, security solution for resisting attacks on link layers are based on spread spectrum while error correcting codes are used in solving threats problem on link layer. All the secure routing schemes [21]-[22] addresses network layer security problem. Usage of cryptographic-based approach was mainly found to be implemented over transport layer security.

ISSN: 2233-7857 IJFGCN

Finally, adoption of intrusion detection system and firewalls are reported to be effective over application layers. The attacks modification are also further classified into various mechanism that uses route sequence number, hop count, changing the source route, tunneling, etc. [23] likewise, reducing another attacking mechanism is based on crowding and overflow of routing chart, fake information broadcasting, and corrupted or manipulated route error message.

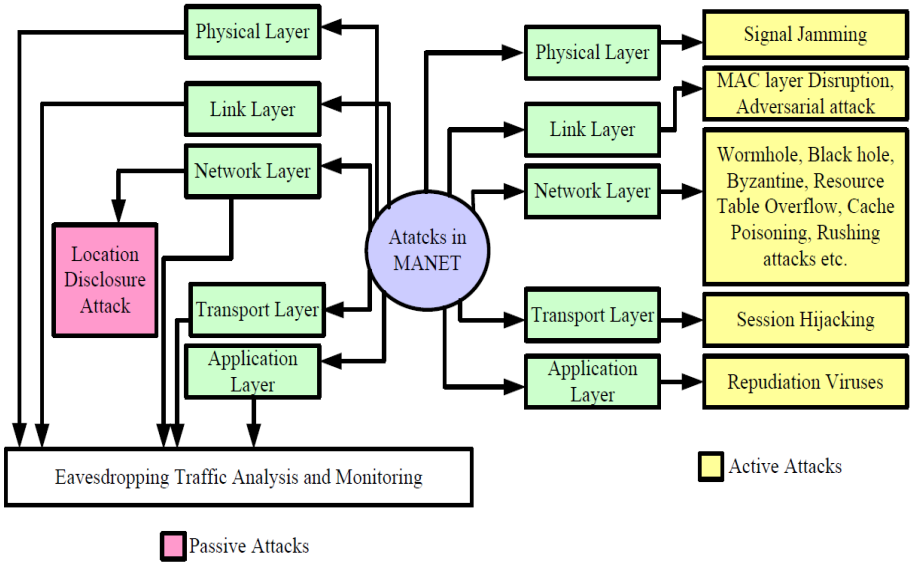

Fig.3. Classification of Attacks in MANET [24]

4. Security Propositions in MANETS

While operating in MANET, it exhibits different security threats at each layer of protocol. To control them various methods are used. As these approaches are fulfilling the security needs at each layer of protocol in MANET. In MANET security measures can be attained through either by key management schemes, Intrusion Detection System (IDS) or secure routing.

4.1 Key Management Schemes

Key management deals with its distribution, its restoration and decision. Various security threats can be recognized in the time, before leading to large scale attacks. It can be achieved through various keys generation schemes for encryption, decryption and Message Authentication Codes (MAC) generation for node authentication and data freshness. Many proposals have used the cryptography keys whether symmetric or asymmetric in Ad hoc networks. The network key, group key or pair wise keys are used to address network level, group level or node-to-node interaction respectively. In a network for securing the information exchange if single key is used, it is classified as network key. When a group of mobile nodes in MANETs are assigned a single key then it is called as group key. Group keying is handled by a group of logical or physical neighbor nodes, as the nature of generation of group keys, its distribution and revocation is a distributed operation [25]. On the basis of different environments as centralized, distributed and decentralized group keying can be classified.

ISSN: 2233-7857 IJFGCN

4.2 Intrusion Detection System (IDS)

An approach for attack detection is called as Intrusion Detection System (IDS). IDS [26] [27] can either Rule Based or Signature Based and Anomaly based Detection. In Rule based way the intrusion is detected by differentiating the signatures against the signatures in data base. The characteristics of signature data base and missing entries in case of the new attacks cannot be classified as intrusion. In an Anomaly based system, the detection is made if any deviation from the normal behavior in traffic patterns, energy consumptions or delays in acknowledgement are compared.[28],[29],[30] ,[31]. The reviewed solutions can be classified at the same time in IDS category as secure routing solutions. A proposal in [32] is used to detect anomaly by calculating the difference in terms of forwarding behavior from the normal behavior. In [33] an IDS for reactive routing schemes is proposed.

5. Problems in Existing MANET Security Solution

In present scenario, there are many different standard routing approaches in MANET that are mainly dedicated for contributing to security solution. Below is a Table no.1 that highlights various important features of security solutions for improving the quality of MANET system. A simple comparative analysis of most frequently used secure routing schemes are is tabulated. All these security schemes are considered as standard solution; however, all of them are also reported to suffer from significant problems. Irrespective of potential capability of resisting tampered and impersonating messages, SAODV [34] uses method of public key encryption, thereby creating overhead in the network. The node that is using Secure AODV is not capable of recognizing any malicious code and due to this such code is also found to be undetected and forwarded to the node at receiving node. Next frequently discussed is SEAD [35] which can resist multiple attackers as well as various other forms of attacks too. It also offers resource cost effective solution towards security. However, it has potential on performing authentication by identifying from neighboring node which utilizes hash chain at faster pace. SDSDV [36] is known for its data integrity, but it also offers significant network overhead. SLSP [37] offers better resistivity towards denial of service attack, but it cannot withstand colluding attack. Secure protocol which is durable to Byzantaine failures (SPRBF) and provides resistance from byzantine failure. Although, it has quite complex implementation cycle to design [38]. SRP [39] is known for its discovery of correct path in vulnerable network; however, it doesn't uses encryption over its routing channel and thereby they cannot resist invisible node attack. ARAN [40] offers robust network structure with supportability of public key encryption; however, it offers higher processing overhead. Finally, SPAAR [41] suffers from stale certificate issues. Therefore, it can be seen that existing standard secure routing schemes cannot be applied for securing upcoming application of MANET that needs dynamic security.

The process of quantification of the threats and different form of adversaries are witnessed very frequently in current times as there are various forms of anomalies and fatal applications [42]. It is reported that there are approximately 10,000 alerts of security almost every day in North America [43]. In this regard, MANET application can be a significant victim which has not been explored or reported by anyone till date. Here are the following main reasons why MANET applications are more prone for attacks viz.

MANET applications are basically decentralized architecture and therefore offering security in large scale is highly challenging

I. MANET uses infrastructure free environment in order to perform communication; hence, chances of both internal and external attack is very high in MANET applications,

II. MANET offers cost effective and seamless communication in Internet-of-Things (IoT) and therefore maintaining a seamless and properly synced security protocols is something that has never been reported before. Inclusion of mobility is another significant problem which causes impediment towards offering potential and robust security. It is because such forms of nodes will necessitate repeated security updates on its patches. More rate of velocity of nodes will cause more problems in intermittent link where delay is inevitable thereby causing obstruction in security updates. Syncing security protocol with routing scheme for mobile nodes in MANET while communicating with other nodes is still an open-end problem to be solved.

Table 1 Summary of Existing MANET security solution

Protocols	MAC	Secret Keys	Hash Chain	Digital Signature	Cryptographic mechanism	Verification mechanism
SAODV [18]	-	Key pair with both public & private	Hop count authenticated using one-way hash chain	Signature used by sender to sign message	Public Key Cryptography	Using digital signature
Ariadne [26]	Yes	Sender & receiver shares secret MAC key	Utilizes hash chain to generate TESLA keys for authentication	-	-	MAC based
SDSDV [20]	Yes	Nodes shares pairwise secret key	-	-	-	MAC based
SEAD [19]	-	Secret key generated by hash function	Metric of routing table and sequence number authenticated by one-way hash	-	-	Hash chain verification
SRP [23]	Yes	Secure authentication between destination & source node	-	-	-	MAC based
SLSP [21]	Yes	Uses both private & public pair of key			Threshold-based	MAC-based, threshold-based key certification
SPAAR [25]	-	Key from neighboring group, Uses both private & public pair of key	-	-	Public key cryptography	Public key cryptography-based verification
ARAN [24]	-	Uses both private & public pair of key	-	-	Public key cryptography	Public key cryptography-based verification
SPRBF [22]	-	On-demand generation of secret key using pairwise approach	-	-	-	Using digital signature

6. Research Gaps

After reviewing the existing research contributions for securing communication in MANET, following research gaps can be jotted:

I. Less Effective key management approaches: There is no uncertainty that there are various key management approaches existing in securing MANET [44], however, they are more prone to one kind of attack and doesn't offer much dynamicity towards changing topology of MANET. There are also less evidence towards optimizing key management approach to ensure lightweight security protocol.

II. Less focus on non-anonymity: Non-anonymity or privacy is ever increasing security breach where there is very less effective solution in existing system [45]. There is a requirement of more studies towards non-anonymity if MANET will

need to support upcoming integration with IoT as they will be exposed to larger network with more vulnerability.

III. Less effort in cost effective computational modeling: The existing security schemes have loopholes. However, an enhancement using novel optimization scheme could offer better resistance [46]. Usage of signature is cost effective approach as well as usage of public key encryption is always a better option in MANET. Hence, cost effective modeling could be carried out towards such factors.

IV. Group security is an area which lacks researches: Communication in the form of groups in MANET is not attained in best possible way in recent times. There is a lack of effective modeling toward enhancing the architecture for group communication system for security option in MANET [47] [48]. While, existing works were highlighting some selected attacks, whereas to make stronger group communication system it is needed to ensure the occupancy of some more forms of attacks.

7. Conclusion

In this paper a discussion of the status of existing security-based solutions in MANET is presented. It is now learned that changing functionalities of the MANET concept itself poses as root cause of various problems. After reviewing existing system, it is found that existing security approaches are all associated with technical flaws which let the algorithm to solve one security problem with ignoring some other associated problem. A secure plan toward route security is still a missing gap. A MANET node also drains energy while performing secure communication and hence its energy as well as other resource efficiency is required to be ensured. Nonetheless, there is no such approach which highlights about such claims. Optimization-based approach has been less attempted and more investigation will be required to be realised towards obtaining its security robustness. Our future direction of work will be to develop an intelligence framework to model the comprehensive behavior of a robust and cost- effective security system among mobile nodes.

References

[1] Jagdish Chand Bansal, Kedar Nath Das, Atulya Nagar, Kusum Deep, Akshay Kumar Ojha, “Soft Computing for Problem Solving” SocProS 2017, Volume 1 Springer.

[2] Dharma P. Agrawal, Qing-An Zeng, “Introduction to Wireless and Mobile Systems”, Cengage Learning, Technology & Engineering, pp. 640, 2015.

[3] Alo, Rita Uzoma, Nwokoro Ifeanyi Stanly, and Nkwo Friday Onwe. "Mobile Ad Hoc Network (MANET): Applications, Benefits and Performance Issues in a Global Positioning System." (2018).

[4] Yadav, Preeti, Krishan Kumar, and Mr Tarun Dalal. "Energy Efficiency Comparative Analysis of Different Routing Protocol In MANET for Healthcare Environment." International Journal on Recent and Innovation Trends in Computing and Communication 6, no. 6 (2018): 121-126.

[5] Suman Paul, “Introduction to MANET and Clustering in MANET”, Anchor Academic Publishing, pp. 40, 2016.

[6] Monica et al. “Evaluation of Attacks using different Parameters based on their performance”International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, March 2018, pp. 106-110 © 2018.

[7] Suresh Chandra Satapathy, Siba K Udgata, Bhabendra Narayan Biswal, “Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013”, Springer Science & Business Media, Computers, pp. 564, 2013.

[8] Al-Sakib Khan Pathan, Muhammad Mostafa Monowar, Zubair Md. Fadlullah, “Building Next-Generation Converged Networks: Theory and Practice”, CRC Press, pp. 608, 2013.

[9] Brij B. Gupta, "Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives", CRC Press Business & Economics, pp. 666, 2018.

[10] C.E. Perkins, P.R. Bhagwat, "Highly dynamic destination sequences distance vector routing (DSDV) for mobile computers", Proceedings of ACM SIGCOMM, pp. 234−244,1994.

[11] D.B. Jonhson, D.A. Maltz, "Dynamic Source Routing in Adhoc wireless networks, Mobile Computing", T. Imie Linski and H. Korth, Eds. Kluwer Academic Publishers, Vol. 53, pp. 153−181, 1996.

[12] C.E. Perkins, E.M. Royer, S. Das, "Adhoc on Demand Distance Vector Routing", Proceedings of Second IEEE workshop on Mobile Computing Systems and applications, pp. 90−100, 1999.

[13] V. Park. S. Corson, "Temporally Ordered Routing Algorithm (TORA) version 1", IETF Internet Draft (draft- ietf-manet-tora-spec-04.txt), July 2001.

[14] Reddy, P. Narendra, C. H. Vishnuvardhan, and V. Ramesh. "Routing Attacks in Mobile Ad hoc Networks." International Journal of Computer Science and Mobile Computing 2, no. 5 (2013).

[15] Leigh Armistead, "CIW2007- 2nd International Conference on Information Warfare & Security: ICIW2007", Academic Conferences Limited, pp. 270, 2007

[16] Monika kashap.et.al"Routing issues and challenges for MANETs: A Review" International Journal of Engineering Research & Technology (IJERT)Vol. 2 Issue 10, October – 2013 ISSN: 2278-0181

[17] Amit Kumar et.al"Secure routing proposals in manets: A review" International Journal in Foundations of Computer Science & Technology (IJFCST) Vol.6, No.1, January 2016

[18] Raffaele Giaffreda, Dagmar Cagáňová, Yong Li, Roberto Riggio, Agnès Voisard, "Internet of Things. IoT Infrastructures: First International Summit, IoT360 2014, Rome, Italy, October 27-28, 2014, Revised Selected Papers,Part 2", Springer, pp. 332, 2015

[19] Saha, Debashis, "Advances in Data Communications and Networking for Digital Business Transformation", IGI Global, pp. 358, 2018

[20] Nadeem, Adnan, and Michael P. Howarth. "A survey of MANET intrusion detection & prevention approaches for network layer attacks." IEEE communications surveys & tutorials 15, no. 4 (2013): 2027-2045.

[21] Shashi, and Siddhartha Chauhan. "A novel approach for mitigating gray hole attack in MANET." Wireless Networks24, no. 2 (2018): 565-579.

[22] Mukherjee, Saswati, Matangini Chattopadhyay, Samiran Chattopadhyay, and PragmaKar. "EAER-AODV: Enhanced Trust Model Based on Average Encounter Rate for Secure Routing in MANET." In Advanced Computing and Systems for Security, pp. 135-151. Springer, Singapore, 2018.

[23] Saha, Himadri N., and Prachatos Mitra. "Intelligent Energy Aware Fidelity Based On-Demand Secure Routing Protocol for MANET." International Journal of Computer Network and Information Security 10, no. 4 (2018): 48.

[24] Islam, Noman. (2013). "Security Issues in Mobile Ad Hoc Network".Doi:10.1007/978-3-642-36169-2_2.

[25] Wu, B., Wu, J., & Dong, Y. (2009)." An efficient group key management scheme for mobile ad hoc networks". International Journal of Security and Networks, 4(1-2), 125- 134.

[26] Northcutt, S., & Novak, J. (2002). "Network intrusion Detection". Sams Publishing.

[27] Khan, S., Loo, K. K., & Din, Z. U. (2010). Framework for intrusion detection in IEEE 802.11 wireless mesh networks. Int. Arab J. Inf. Technol., 7(4), 435-440.

[28] Chen, T., Kuo, G. S., Li, Z. P., & Zhu,G.M.(2007)."Intrusion detection in wireless mesh networks"(pp. 146-169).

[29] Rafsanjani, M. K., Movaghar, A., & Koroupi, F. (2008). "Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes" World Academy of Science, Engineering and Technology, 20, 351- 355.

[30] Ramanathan, S., & Steenstrup, M. (1996)."A survey of routing techniques for mobile communications networks". Mobile Networks and Applications, 1(2), 89- 104.

[31] Zeng, Q. A., & Agrawal, D. P. (2002). "Introduction to wireless and mobile systems". CENGAGE Learning.

[32] Macker, J. (1999). Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations.

[33] Forouzan, B. A. (2007). “Cryptography & Network Security”. McGraw-Hill,Inc. Vanitha, K., and AMJ Zubair Rahaman. "Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol." Cluster Computing (2018): 1-9.

[34] Krishnan, Rahul."A Survey on Game Theory Approaches for Improving Security in MANET." American Journal of Electrical and Computer Engineering 2, no.1 (2018):1-4.

[35] Ye, Yongfei, Suqin Feng, Minghe Liu, Xinghua Sun, Ting Xu, and Xuming Tong. "A Safe Proactive Routing Protocol SDSDV for Ad Hoc Network." International Journal of Wireless Information Networks 25, no. 3 (2018): 348-357.

[36] Ojetunde, Babatunde, Naoki Shibata, and Juntao Gao. "Monitoring-Based Method for Securing Link State Routing against Byzantine Attacks in Wireless Networks." Journal of Information Processing 26 (2018): 98-110.

[37] Monica, Lalita Luthra. "Evaluation of Attacks using different Parameters based on their performance." Evaluation 1 (2018): 106-110.

[38] Mandhare, Archana, and Sujata Kadam. "Performance Analysis of Trust-Based Routing Protocol for MANET." In Computing, Communication and Signal Processing, pp. 389- 397. Springer, Singapore, 2019.

[39] Ahmad, Shahnawaz. "Alleviating Malicious Insider Attacks in MANET using a Multipath on-demand Security Mechanism." International Journal of Computer Network and Information Security 10, no. 6 (2018): 40.

[40] Eissa, Tameem, Shukor Abdul Razak, Rashid Hafeez Khokhar, and Normalia Samian. "Trust-based routing mechanism in MANET: Design and implementation." Mobile Networks and Applications 18, no. 5 (2013): 666- 677.

[41] Lin, Derek. "Anomaly detection system for enterprise network security." U.S. Patent 9,112,895, issued August 18, 2015.

[42] Tekade, Pooja, and Nutan Dhande. "Designing Security System for Ring Topology in WSN." (2018).

[43] Thylashri, S., D. Femi, S. Alex David, and A. Suresh. "Vitality and peripatetic sustain cluster key management schemes in MANET." (2018).

[44] Haakensen, Thomas J. “Enhancing sink node anonymity in tactical wireless sensor networks using a reactive routing protocol”. Naval Postgraduate School Monterey United States, 2017.

[45] Lu, Ting, and Jie Zhu. "Genetic algorithm for energy- efficient QoS multicast routing." IEEE Communications Letters 17, no. 1 (2013): 31-34.

[46] Chilveri, P. G., and M. S. Nagmode. "Security Issues in Heterogeneous Network: A review." International Journal of Applied Engineering Research 13, no. 1 (2018): 798- 808.

[47] Manish Devendra Chawhan,Ausaf Umar Khan “A Survey on Cross Layer Framework based Energy Efficient Routing Protocols of Manets” International Journal of Future Generation Communication and Networking Vol. 13, No. 1, (2020), pp. 1125-1135

Authors

ram Nausheen obtained Bachelor of Engineering degree in Electronics and Telecommunication Engineering from Anjuman College of Engineering & Technology,under RTMNU in 2010. She got her Masters’s Degree in Electronics Engineering from G.H.Raisoni College of Engineering under RTMNU in 2013.She has been in teaching profession since 2010.Presently, she is working as Assistant Professor in Department of Electronics and Telecommunication, Anjuman College of Engineering & Technology, Nagpur, Maharashtra and she is a Research Scholar in faculty of Electronics and Communication Engineering at SAGE Universiry ,Indore, Madhya Pradesh. Her research interests are Wireless Communication,Wireless networks, Network Security, Intrusion Detection, Crosslayer design, Mobie Adhoc networks(MANET)