Insights on Security Improvements and Implications of Artificial Intelligence in MANET

Shivashankar T. M.
Research Scholar,
Visvesvaraya Technological University, Belagavi,
Karnataka, India

S. B. Shivakumar
Professor, Department of Electrical & Electronics,
RYM Engineering College,
Bellary, Karnataka, India

ABSTRACT

Mobile Adhoc Network (MANET) is claimed to be an integral part of all futuristic network and communication system e.g. cloud, reconfigurable network, Internet-of-Things (IoT), inter-domain routing, etc. However, the security problems of MANET is not yet been mitigated irrespective of archives of security approaches and solution. For a MANET system to be integrated with upcoming technologies it is required that their routing system should offer higher level of resistance against all potential threats as well as they should also offer a better flexibility to tailor the security scheme based on demand of the environment, where the mobile nodes are operating. It is also seen that Artificial Intelligence is another big boon which is currently being proliferating at faster speed and there are some segment of research where it is also claimed to contribute towards security system in MANET. Therefore, this paper offers insights to the current state of security system using conventional as well as using Artificial Intelligence to explore about its research gap.

Keywords

Mobile Adhoc Network, Security, Artificial Intelligence, Encryption, Robustness

1. INTRODUCTION

Mobile Adhoc Network (MANET) has been a consistent focus among the research community from past decade owing to its cost effective beneficial features associated with communication [1] [2]. Due to lack of infrastructure, MANET is known to offer faster communication performance over its unorganized environmental condition. Irrespective of various applications of MANET [3] [4], they have many pitfalls too. The prime reason of the challenges associated with MANET is its decentralized architecture and its dynamic topology causing random alterations over the routing information [5]. The prominent causes of the security loopholes in MANET are i) absence of efficient and robust resistance from adversary, ii) fair chances of presence of lethal threats within a network, iii) no centralized management, iv) fluctuating scalability, v) highly constraint of energy factor within the node, etc [6]. Till date, it is being explored that approaches towards security in MANET is basically of two types. The *first* type is related to securing routing scheme [7] and *second* type is related to data security scheme [8]. 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 focused on resisting adversary from invoking intruders. The usage of key-agreement protocols are not much supported in MANET owing to absence of any infrastructure. Moreover, it is very unlikely to establish a trust-based factor within the mobile nodes. Moreover, such forms of wireless communication channel are highly prone to intrusion owing to different routing-based attacks [9]. 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. Normally, it was seen that attack strategy are of two types viz. i) attacks towards outbound data and ii) attacks towards core operations of mobile nodes. However, basically the standard classification is for only two types viz. internal and external attacks [10]. Further, it has been seen that external intrusion 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. Researchers believed that internal attacker is the most challenging form of intrusion in MANET and very difficult to identify as well as resist it. Such form of attack could perform illegitimate broadcasting of forged information of routing to neighboring mobile nodes in such a way that one regular node is totally under the control of attacker. Such captivated regular node is termed as *compromised mobile node* or internal attacker. Such node bears the capability of generating legitimate signature with an aid of private keys. However, the presence of dynamic topology will further worsen the scenario. On the other hand, passive attack is about obtaining sensitive information in stealth mode from the routing operation. The purpose of passive attack is to disclose the confidential information to the attacker that could let the adversary control the sensitive information of the mobile nodes.

Although, there has been various dedicated approaches toward securing MANET applications, but still the security problems are at large. The prime contribution of this paper is to brief the problems associated with existing security solution in MANET as well as to promote the usage of Artificial Intelligence in order to offer robust security. The idea is to extract the research gap. The organization of this paper is as follow: Section-2 discusses about the significance of MANET security followed by discussion of problems associated with existing security solution in Section-3. Section-4 presents a discussion of the evolution of Artificial Intelligence towards adhoc network security while explored research gap is presented in Section-5. Section-6 offers conclusive remarks of the review paper.

2. SIGNIFICANCE OF MANET SECURITY

At present, MANET and its application are seeked upon as an essential part of an on-going technology called as Internet-of-Things (IoT). Several literatures e.g. [11] has already discussed that MANET is one of the essential domain of communication in IoT as it offers infrastructure-free communication system with mobility. It will mean that IoT which uses a massive network of cloud to offer data availability will now offer processing and analyzing with mobile nodes if MANET is used in IoT. This has got lot of advantage e.g. faster rate of data processing and application, better redundancy management, and supportability of time-bound emergency services. However, the challenging part of it will be to offer robust security protocol as MANET will be now exposed to exponentially large network which is prone to trillions of malwares due to usage of internet [12]. 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 IoT system, than there are also inclusions of different heterogeneous routing scheme which will surely affect the communication process too. Therefore, MANET security is definitely not an easy way to achieve.

A significant problems associated with existing literature is that different literature shows different forms of classification of intrusion in MANET. According to Nadeem and Howarth [13], it was said that attacks in MANET are normally of two types 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 Gurung and Chauhan [14] discussed that flooding attack is the most lethal among all and hence the authors have presented classification of flooding attack as two types viz. continuous attack (ASRRF[14], NASRRF[14]) and selective attack (ASDF [14], NASDF [14]). Fig.1 highlights the standard taxonomies of lethal attacks reported in MANET with respect to different 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, 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 attack attacks on network layer. Transport layer only witnesses session hijacking as the active model of attacks in MANET while application layer suffers from reputation, Trojans, malwares, virus, etc as the mode of active attacks.

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 [15]-[16] addresses network layer security problem. Usage of cryptographic-based approach was mainly found to be implemented over transport layer security. Finally, adoption of intrusion detection system and firewalls are reported to be effective over application layers. Existing research work also offers emphasize that intrusion due to illegitimate modification or protocol or system and fabrication of message are another challenging security problems in MANET. The attacks bas edon modification are also further classified into various mechanism that uses route sequence number, hop count, changing the source route, tunneling, etc. Similarly, attacking principle using fabrication is based on overflow of routing table, forged information broadcasting, and corrupting / manipulating route error message.

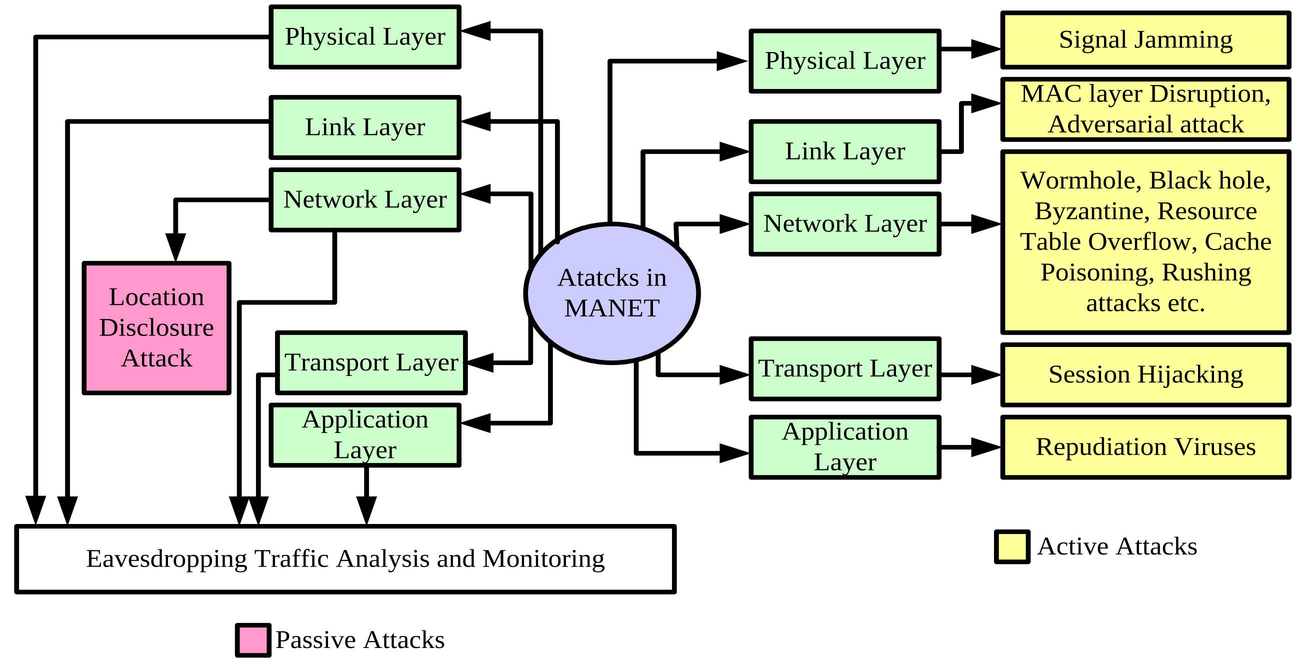

Figure 1 Standard taxonomy of attack in MANET [17]

3. PROBLEMS IN EXISTING MANET SECURITY SOLUTION

At present, there are various standard routing schemes in MANET that is dedicated only for offering security using various approaches. Table 1 highlights various essential features of security solution for strengthening the MANET system. A simple comparative analysis of most frequently used secure routing schemes 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 [18] uses public key encryption, thereby imposing overhead. The node using SAODV is not capable of identifying any malicious code and hence such code is also forwarded undetected to receiver node. Next frequently discussed is SEAD [19] 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 dependencies on performing authentication from neighboring node which consumes hash chain in faster rate. SDSDV [20] is known for its data integrity, but it also offers significant network overhead. SLSP [21] offers better resistivity towards denial of service attack, but it cannot withstand colluding attack. Secure protocol resilient to Byzantaine failures (SPRBF) offers resistance from byzantine failure; however, the implementation cycle of it is quite complex to design [22]. SRP [23] 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 [24] offers robust network structure with supportability of public key encryption; however, it offers higher processing overhead. Finally, SPAAR [25] 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.

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

4. EVOLUTION OF AI IN SECURITY

From the prior section, it can be seen that there are various existing approaches contributing towards the security of MANET. Out of all the techniques, it has been observed that Artificial Intelligence (AI) is one of the upcoming concepts embedded in different network technologies and communication system. Basically, AI is a mechanism of converting various devices connected a very smart and intelligence. The essential contribution of AI is to make the system takes autonomous decision just like human's intelligence system [27]. The implementation of AI dates back on 1990 when it was reported to be used in scheduling, gams, reasoning, mining, natural language processing, etc [28]. The backbone of the AI is constructed on the basis of multiple discipline e.g. mathematics, biology, computer, linguistic, and engineering. The prime concept of the AI is to perform an organization of the data and system in order to ensure that i) there should be maximum perceptibility for the user who also offers data, ii) the data or system should be subjected to modification in order to rectify the errors, and iii) it should offer higher utilization irrespective of the fact that it could offer some error-prone information [29]. At present, the concept of AI is categorized into machine learning, natural language processing, speech system, expert system, robotics, and vision [30].

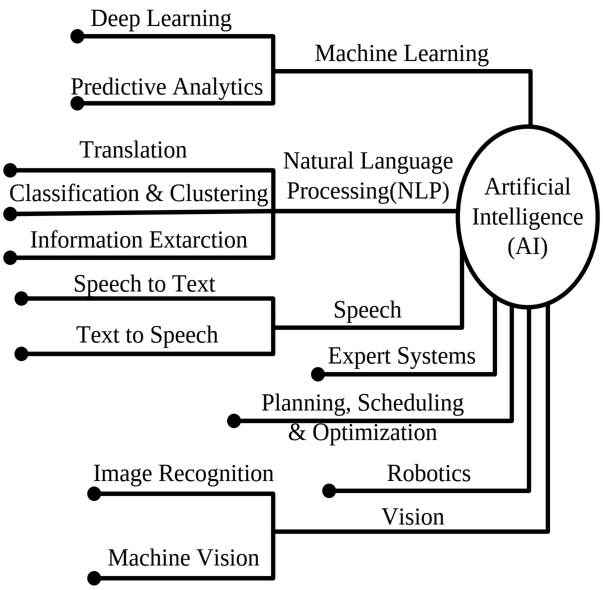

Figure 2 Classification of AI

Apart from security, different approaches of AI are already reported to be used in enhancing operation of wireless network system. Usage of Q-learning [31], learning automata [32], Neural Network [33] are already reported to improve the routing performance in wireless network. Similarly, Bayesian learning [34] and k-means clustering [35] are found to improve the channel capacity of wireless network. From security viewpoint, AI is also reported to be used in designing intruder detection system e.g. usage of decision tree [36] and perceptron-based approach [37-38] was used for securing communication system in wireless networks. Similarly, usage of Principal Component Analysis is used for ensuring fault tolerance as well as higher integrity in the communication system of wireless networks.

From the commercial utilization viewpoint, some of the currently existing commercial security tools that uses AI are i) Symantec Targeted Attack Analytics tool [39], ii) Sophos Intercept X tool [40], iii) Darktrace Antigena [41], iv) IBM QRadar Advisor [42], v) Vectra Cognito [43], etc. From cyber-security viewpoint, AI is becoming an essential demand in current times. Following are the justification behind adoption of AI in offering higher security of networks:

- *Managing Massive data volume*: Owing to massive generation of data from varied log files, system-generated alerts, etc, it is quite a challenging task to secure such exponential data with higher complexity. Usage of AI could offer better data selection to ease off the complexity associated with offering precise data security which is manually impossible for humans.
- *Effectively exposes the threats*: Usage of AI could offer accurate and faster exploration of the adversary present in the network. AI offers potential to learn the behaviour of both users as well as network in order to incorporate more intelligence for an effective decision making towards determining the lethal of fatality for any threats.
- *Faster Response Time*: Be it security or any other problem, AI offers much efficiency in the processing it. Utilization of multiple available alert system as well as secure data logs are utilized for speeding the process of threat analysis.
- *Illegitimate Usage of AI*: The usage of AI is very much dangerous if they are used by the attacker. They can be deployed in the network or device where various confidential and private information are at stake. Hence, usage of AI by adversary offers more damage than compared to usage of AI for beneficial purpose.

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 [44]. It is reported that there are approximately 10,000 alerts of security almost every day in North America [45]. In this regard, MANET application can be a significant victim which has not been explored or reported by anyone till date. Following are the reasons why MANET applications are more prone for attacks viz. i) MANET applications are basically decentralized architecture and therefore offering security in large scale is highly challenging, ii) MANET uses infrastructure free environment in order to perform communication; hence, chances of both internal and external attack is very high in MANET applications, iii) 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 require frequent 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. Hence, there are various security problems that are yet to be investigated to find if AI can offer solution.

Irrespective of different taxonomies of the field of implications of AI, there are only few approaches of AI that has been reported to be utilized for securing network system. Briefing of existing AI based security approaches are as follow;

i) Fuzzy-Logic based Security Solution

Usually Fuzzy logic is applied in the scenario where the input parameters are either vague or impartial. Using a significant inference rule, it can be suitably used for carving security demands as per expectation. The most recent work of Zhang et al. [46] have combined fuzzy logic and swarm optimization concept in order to develop a secure routing protocol for vehicular networks. Using a simulation-based study, the study outcome shows effective packet forwarding performance over increasing mobile nodes. A slightly different concept of fuzzy logic was implemented by Theresa and Sakthivel [47] where a two stage fuzzy logic for identification of threat and controlling of it is introduced. Hiremath et al. [48] have presented a solution towards resisting blackhole attack using fuzzy logic. The idea is to offer an enhanced on-demand routing protocol more secure adaptively. Similar line of research work is also carried out by Balan et al. [49]. The work carried out by Inaba et al. [50] emphasizes on the improving the handover policy as well as call admission control by incorporating security approach. The construction of the model is carried out by involving various new parameters that are based on distance, angle, and mobility over the mobile nodes in MANET. Fuzzy logic is used for developing the control system on the basis of the above mentioned parameters. The study outcome is all about the decision value that is capable of identification of the intruders with high precision. A trust-based security approach was reported in literature by Xia et al. [51] where the core idea is to track the malicious node and thereby resist attacks in MANET. Fuzzy logic was used in this work for constructing policies for trust factor and offering a better form of inference system in order to compute the trust of the node. The analysis of the study was carried out with simulation-based approach where presented system has been proven to offer better trust value compared to other existing trust-based approaches. Further work towards enhancing the fuzzy-based rules for improving the security strength of the system associated with the MANET is carried out by Khatri et al. [52]. The authors have implemented dual-level fuzzy logic system in order to determine the level of trust for the mobile nodes.

ii) Neural Network based Security Solution

Neural network is another frequently used approach of Artificial intelligence reported towards securing the MANET system. Apart from multiple beneficial feature of neural network, some of the important feature of neural network that can be harnessed for securing MANET are i) the learning algorithms in neural network can be used for obtaining the most suitable scenario of higher security strength, ii) the adoption of multiple and different inputs for the processor (or neuron) is another best feature that can be used for modeling the security solution in MANET, where multiple and different constraints can be used as well as its outcomes could be also controlled to higher extent. There are some significant research attempts towards utilizing neural network for strengthening the security system in MANET. Most recently, the work carried out by Brun et al. [53] have make use of the advanced version of the neural network i.e. deep learning approach for the purpose of identifying the security threat in MANET. The authors have used random neural network for this purpose using empirical approach considering the case study of the Internet-of-Things as MANET is considered as one of the integral part of it. The presented logic is about capturing the flow of the data from the heterogeneous network devices over gateway system which are also connected with the cloud system. The application of this algorithm is carried out over the captured packets using various forms of metrics for performing real-time identification of the threat. The presented approach has used experimental approach where python scripting was carried out towards attack detection. However, the study was only limited to few forms of attacks only. Neural network as well as genetic algorithm has also been reported to improve the attack identification system in MANET. The work in this direction was carried out by Elwahsh et al. [54] has jointly utilized self-organizing map as well as genetic algorithm where the preference is offered more on the unsupervised learning approach in order to explore the best possibility of initial-reported cases of intrusion as per the assigned fitness function. Another interesting part of this study is that it emphasizes on the uncertain behaviour of the adversaries. The concept of the deep learning has been re-investigated by Koesdwiady et al. [55]. Although, the study was not directly associated with the security loopholes in MANET, but it emphasizes on working on different parameters of the mobile network where harnessing deep neural network has better implications towards system design. Implication of the intelligence-based approach carried out towards resisting specific form of attack. Work in such direction was carried out by Alheeti et al.[56]. A modeling was carried out considering the vehicular network where the security features has been escalated using support vector machine and feed-forward neural network. The prime idea of this work is to resist the rushing and grey hole attack. Solution towards similar forms of attacks has also been carried out by Divya [57]. The authors have used neural network as well as an unique sampling technique on the basis of trace-back features in order to resist the most fatal threat i.e. denial-of-service. The idea of the presented logic has been carried out using simulation-based approach using packets and energy as performance parameters. An unique trust-based security approach was formulated by the Liu et al.[58] where the target was to offer sufficient security of the messages being transacted by MANET. The presented system was in support of encryption and uses neural network for facilitating secure and multi-path communication in MANET. The study implements MAC protocol 802.11 where a simplified computation of trust factor is carried out to prove that presented solution offer better response time with effective computation of trust even with increasing number of nodes. Similar line of implementation is also carried out by Moradi et al. [59] for resisting denial-of-service attack using neural network. These are the only work carried out using neural network for strengthening the security system in MANET.

i*ii) Machine Learning based Security Solution*

Machine learning-based approach is another frequently used approach towards boosting the security features in MANET. One of the significant advantages of Machine Learning-based approach is that it enhances the efficiency as well as accuracy of the data over a period of time. There are certain research works being carried out using machine learning approach towards securing the communication system in MANET. Most recent discussion carried out by Luong et al. [60] have stated that there are some significant contribution of using machine learning towards resisting flooding attack in MANET. The authors have presented a solution towards identified the illegitimate access request by the mobile nodes by using n unique historical routing data for assisting in offering more insights towards malicious behaviour of nodes. The presented technique makes use of k-nearest neighboring algorithm for this purpose of resisting the flooding-based attacks in MANET. Another recent work of Dadras et al. [61] have used machine learning approach for resisting control modification attacks as well as system identification process also. The idea encouraged the implication of machine learning approach towards system identification but doesn’t address dynamic attack. Usage of machine learning towards modeling intelligence in mobile network has witnessed various forms of approaches in existing times. The work of Liang et al. [62] has strongly advocated that utilization of machine learning in vehicular network and it also discusses about different process of constructing intelligence. According to the author, there are still open-end problems associated with security problems in MANET and its solution using machine learning approach e.g. complexity in method, usage of discrete signals in vehicular network, etc. Similar research problem has been considered in the work of Zhang et al. [63] where machine learning has been used for preserving the privacy of the data. Different from other studies, this implementation scheme makes use of the dynamic learning system over distributed data from log files of vehicles. The input is subjected to pre-processing followed by forwarding the preprocessed data to the local detection engine. However, in order to perfectly work, the proposed system makes an interactive bridge between learning algorithm and privacy preservation techniques. This secondary input further offers more intelligence to raise a correct alarm. Similarly, there are many literatures that emphasize that learning-based approaches offers more edge to the security feature in MANET. The work of Peterson et al. [64] has used machine learning for presence of intruder on online communication in MANET thereby assisting in processing event information of complex origin. It is also known that presence of fault also invites various security threats. This logic has been investigated by Sargolzaei et al. [65] where the emphasis is towards developing a decision system for supporting identification of system fault in cyber-physical system of vehicular network.

Table 1 offers compact version of all the significant review of existing artificial intelligence-based security solutions toward safeguarding communication process in MANET.

Table 1 Summary of Existing AI-based Security Solution

Authors	Problems	Techniques	Advantages	Limitation
Zhang et al. [46]	Securing vehicular network	Fuzzy Logic, ant colony optimization	Effective for both single/multiple attack	-smaller simulation environment, highly recursive
Theresa and Sakthivel [47]	Intrusion detection	Two stage fuzzy logic	Highly adaptive	-restrictive to traffic with constant bit rate
Hiremath et al. [48], Balan et al. [49]	Intrusion detection & prevention, blackhole attack	Adaptive fuzzy	Adaptive charecteristics	Attack specific solution
Inaba et al. [50] emphasizes	Secure routing	Unique interfacing using Fuzzy logic	Connection availability	Less focus on analysis on security strength
Xia et al. [51]	Trust management	Trust-based fuzzy rules	Can be used for comprehensive attack identification	Accuracy on trust over dynamic attacks not discussed.
Khatri et al. [52]	Trust management	Dual-level fuzzy logic	Better trust level	Less extensive analysis
Brun et al. [53]	Attack identification	Deep Learning, Random neural network	Predictive approach	Attack specific solution, computational complexity not evaluated
Elwahsh et al. [54]	Classification of adversary	Genetic algorithm, self-organizing map	Can identify unknown attack	computational complexity not evaluated
Alheeti et al.[56]	Security of vehicular network	Feed-forward, support vector machine	Better communication performance	Specific solution for grey hole and rushing attack.
Divya [57]	Security channeling in sensitive mobile nodes	Neural network, sampling	Can resist IP spoofing	Resistive against denial-of-service only
Liu et al.[58]	Trust management	symmetric block cipher, neural network	Reduced selection of route,	Needs more epoch for better result
Moradi et al. [59]	Denial of service attack	Feed-forward, back propagation	Simplified model	Specific to denial-of-service attack
Luong et al. [60]	Flooding attack in MANET	K-nearest neighboring	Higher accuracy of attack identification	Not resistive towards dynamic attack
Dadras et al. [61]	Detection of control modification attack	System identification, machine learning	Simple and efficient system	Not resistive towards dynamic attack
Zhang et al. [63]	Privacy factor	Distributed learning system	Supports optimization	Dependent upon training dataset
Peterson et al. [64]	Intrusion detection	Support Vector Machine	Simplified classification	Not resistive towards dynamic attack
Sargolzaei et al. [65]	Fault detection	Decision support system	Reliable and robust	System complexity not assessed.

5. OPEN RESEARCH ISSUES

After reviewing the existing research contributions towards securing communication in MANET, following research gaps are explored:

- *Less Effective key management approaches*: There is no doubt that there are various key management approaches existing in securing MANET [66], 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.

- *Less focus on non-anonymity*: Non-anonymity or privacy is ever increasing security breach where there is very less effective solution in existing system [67]. There is a need 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.
- *Less effort in cost effective computational modeling*: There is no doubt there existing security schemes have pitfalls, however, a deliberate enhancement using novel optimization scheme could offer better resistance [68]. 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.
- *Lack of studies on forced group security*: Group communication in MANET is just an option and that has not received much better attention in existing times. There is no effective modeling approach toward even enhancing the architecture towards group communication system for better security option in MANET [69]. Moreover, existing work is focused on specific attacks, whereas strengthening group communication system will ensure covering some more forms of attacks.
- *Nascent Stage of usage of Artificial Intelligence*: Artificial Intelligence has many potentials to incorporate intelligence to the security system [70]. However, the work towards using artificial intelligence is just a beginning and none of the work using artificial intelligence towards security has even been proven using benchmarking nor they have been proven to be resistive against dynamic form of attack.

6. CONCLUSION

This paper has presented a discussion of the status of existing security-based solutions in MANET. It is now learned that inherent 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 comprehensive security 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. However, there is no such approach which highlights about such claims. Optimization-based approach has been less attempted as well as Artificial Intelligence is just a beginning and more investigation will be required to be carried out towards harnessing its smart-intelligence building capability towards invoking security robustness. Our future direction of work will be to develop an intelligence framework where artificial intelligence will be used to model the comprehensive behaviour of a robust and cost-effective security system among mobile nodes.

7. 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] 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

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

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

[9] 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).

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

[11] 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

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

[13] 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.

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

[15] Mukherjee, Saswati, Matangini Chattopadhyay, Samiran Chattopadhyay, and Pragma Kar. "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.

[16] 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.

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

[18] Vanitha, K., and AMJ Zubair Rahaman. "Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol." Cluster Computing (2018): 1-9.

[19] 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.

[20] 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.

[21] 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.

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

[23] 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.

[24] 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.

[25] 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.

[26] Ching-Hsien Hsu, Laurence T. Yang, Jianhua Ma, Chunsheng Zhu, "Ubiquitous Intelligence and Computing: 8th International Conference, UIC 2011, Banff, Canada, September 2-4, 2011, Proceedings", Springer Science & Business Media,, pp. 592, 2011

[27] Elwahsh, Haitham, Mona Gamal, A. A. Salama, and I. M. El-Henawy. "A Novel Approach for Classifying MANETs Attacks with a Neutrosophic Intelligent System based on Genetic Algorithm." Security and Communication Networks 2018 (2018).

[28] Silva, Vivian, Jelena Mitrovic Santos, and Siegfried Handschuh. "WordNetGraph: Structuring WordNet Natural Language Definitions."

[29] Upadhyay, Saurabh, and Aruna Bajpai. "Avoiding Wormhole attack in MANET using statistical analysis approach." International Journal on Cryptography and Information Security 2, no. 1 (2012): 15-23.

[30] Berg, Markus M. "Modelling of natural dialogues in the context of speech-based information and control systems." (2014).

[31] Vijaya Kumar, Anitha, and Akilandeswari Jeyapal. "Self-adaptive trust based ABR protocol for MANETs using Q-learning." The Scientific World Journal 2014 (2014).

[32] Misra, Sudip, P. Venkata Krishna, Akhil Bhiwal, Amardeep Singh Chawla, Bernd E. Wolfinger, and Changhoon Lee. "A learning automata-based fault-tolerant routing algorithm for mobile ad hoc networks." The Journal of Supercomputing 62, no. 1 (2012): 4-23.

[33] Mandal, Jyotsna Kumar, Goutam Saha, Debdatta Kandar, and Arnab Kumar Maji, eds. Proceedings of the International Conference on Computing and Communication Systems: I3CS 2016, NEHU, Shillong, India. Vol. 24. Springer, 2018.

[34] Loo, Jonathan, Jaime Lloret Mauri, and Jesus Hamilton Ortiz, eds. Mobile ad hoc networks: current status and future trends. CRC Press, 2016.

[35] Karmore, Preetee K., and Smita M. Nirkhi. "Detecting Intrusion on AODV based Mobile Ad Hoc Networks by k-means Clustering method of Data Mining." International journal of computer science and information technologies 2, no. 4 (2011): 1774-1779.

[36] Bu, Shengrong, F. Richard Yu, Xiaoping P. Liu, Peter Mason, and Helen Tang. "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks." IEEE transactions on vehicular technology 60, no. 3 (2011): 1025-1036.

[37] Anzer, Ayesha, and Mourad Elhadef. "A Multilayer Perceptron-Based Distributed Intrusion Detection System for Internet of Vehicles." In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), pp. 438-445. IEEE, 2018.

[38] Meng, Guozhu, Yang Liu, Jie Zhang, Alexander Pokluda, and Raouf Boutaba. "Collaborative security: A survey and taxonomy." ACM Computing Surveys (CSUR) 48, no. 1 (2015): 1.

[39] Jenab, Kouroush, and Saeid Moslehpour. "Cyber security management: A review." Business Management Dynamics 5, no. 11 (2016): 16-39.

[40] Ruiz-Heras, A., Pedro García-Teodoro, and Leovigildo Sánchez-Casado. "ADroid: anomaly-based detection of malicious events in Android platforms." International Journal of Information Security 16, no. 4 (2017): 371-384.

[41] Song, Kevin, Paul Kim, Vedant Tyagi, and Shivani Rajasekaran. "Artificial Immune System (AIS) Based Intrusion Detection System (IDS) for Smart Grid Advanced Metering Infrastructure (AMI) Networks." (2018).

[42] Gut, Alain, and Andreas Wespi. "Increasing the Efficiency of Security Analysts." In Cybersecurity Best Practices, pp. 349-361. Springer Vieweg, Wiesbaden, 2018.

[43] Oprea, Alina, Zhou Li, Robin Norris, and Kevin Bowers. "MADE: Security Analytics for Enterprise Threat Detection." In Proceedings of the 34th Annual Computer Security Applications Conference, pp. 124-136. ACM, 2018.

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

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

[46] H. Zhang, A. Bochem, X. Sun and D. Hogrefe, "A Security Aware Fuzzy Enhanced Reliable Ant Colony Optimization Routing in Vehicular Ad hoc Networks," 2018 IEEE

Intelligent Vehicles Symposium (IV), Changshu, 2018, pp. 1071-1078.

[47] W. G. Theresa and S. Sakthivel, "Fuzzy based intrusion detection for cluster based battlefield MANET," 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Chennai, 2017, pp. 22-27.

[48] P. S. Hiremath, Anuradha T and P. Pattan, "Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs," 2016 International Conference on Information Science (ICIS), Kochi, 2016, pp. 245-251.

[49] Balan, E. Vishnu, M. K. Priyan, C. Gokulnath, and G. Usha Devi. "Fuzzy based intrusion detection systems in MANET." Procedia Computer Science 50 (2015): 109-114.

[50] T. Inaba, D. Elmazi, Y. Liu, S. Sakamoto, L. Barolli and K. Uchida, "Integrating Wireless Cellular and Ad-Hoc Networks Using Fuzzy Logic Considering Node Mobility and Security," 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangiu, 2015, pp. 54-60.

[51] H. Xia, Z. Jia, L. Ju, X. Li and Y. Zhu, "A Subjective Trust Management Model with Multiple Decision Factors for MANET Based on AHP and Fuzzy Logic Rules," 2011 IEEE/ACM International Conference on Green Computing and Communications, Sichuan, 2011, pp. 124-130.

[52] P. Khatri, S. Tapaswi and U. P. Verma, "Fuzzy based trust management for wireless ad hoc networks," 2010 International Conference on Computer and Communication Technology (ICCCT), Allahabad, Uttar Pradesh, 2010, pp. 168-171.

[53] Brun, Olivier, Yonghua Yin, Erol Gelenbe, Y. Murat Kadioglu, Javier Augusto-Gonzalez, and Manuel Ramos. "Deep learning with dense random neural networks for detecting attacks against iot-connected home environments." In Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Lecture Notes CCIS, no. 821. 2018.

[54] Elwahsh H, Gamal M, Salama AA, El-Henawy IM. A Novel Approach for Classifying MANETs Attacks with a Neutrosophic Intelligent System based on Genetic Algorithm. Security and Communication Networks. 2018;2018.

[55] A. Koesdwiady, R. Soua and F. Karray, "Improving Traffic Flow Prediction With Weather Information in Connected Cars: A Deep Learning Approach," in IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 9508-9517, Dec. 2016.

[56] Ali Alheeti, K.M., Gruebler, A. and McDonald-Maier, K., 2016. Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks. Computers, 5(3), p.16.

[57] Divya, D. "Intrusion Detection in MANET using Neural Networks and ZSBT." International Journal of Computer Applications 81, no. 4 (2013).

[58] C. Liu, I. Woungang, H. Chao, S. K. Dhurandher, T. Chi and M. S. Obaidat, "Message Security in Multi-Path Ad Hoc Networks Using a Neural Network-Based Cipher," 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, Kathmandu, 2011, pp. 1-5.

[59] Moradi, Zahra, Mohammad Teshnehlab, and Amir Masoud Rahmani. "Implementation of neural networks for intrusion detection in manet." In Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on, pp. 1102-1106. IEEE, 2011.

[60] Luong, N.T., Vo, T.T. and Hoang, D., 2019. FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks. Wireless Communications and Mobile Computing, 2019.

[61] S. Dadras, S. Dadras and C. Winstead, "Identification of the Attacker in Cyber-Physical Systems with an Application to Vehicular Platooning in Adversarial Environment," 2018 Annual American Control Conference (ACC), Milwaukee, WI, 2018, pp. 5560-5567.

[62] L. Liang, H. Ye and G. Y. Li, "Towards Intelligent Vehicular Networks: A Machine Learning Framework," in IEEE Internet of Things Journal.

[63] T. Zhang and Q. Zhu, "Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs," in IEEE Transactions on Signal and Information Processing over Networks, vol. 4, no. 1, pp. 148-161, March 2018.

[64] E. Petersen, M. A. To and S. Maag, "A novel online CEP learning engine for MANET IDS," 2017 IEEE 9th Latin-American Conference on Communications (LATINCOM), Guatemala City, 2017, pp. 1-6.

[65] A. Sargolzaei, C. D. Crane, A. Abbaspour and S. Noei, "A Machine Learning Approach for Fault Detection in Vehicular Cyber-Physical Systems," 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, 2016, pp. 636-640.

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

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

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

[69] 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.

[70] Garg, Rajni, and Vikas Mongia. "Mitigation of Black Hole Attack in Mobile Ad-Hoc Network Using Artificial Intelligence Technique." (2018).