Machine Learning Based Security Solutions in MANETs:
State of the art approaches

Renu Popli¹, Monika Sethi², Isha Kansal³, Atul Garg⁴ and Nitin Goyal⁵
Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India
E-mail: renu_popli@yahoo.co.in

Abstract. Machine learning (ML) techniques provide the learning capability to a system and encourage adaptation into the environment, based upon many logical and statistical operations. The prime goal of ML is to recognize the complex patterns and make decisions based on the results. There are various ML algorithms which are implemented to secure the mobile ad-hoc networks. The infrastructure-less environment of MANETs poses a great challenge in implementation of the security systems. The security approaches in MANETs mainly focus on intrusion detection, malicious attacks mitigation, elimination of outlier/misbehavior/selfish nodes and securing routing paths. The researchers have been using cutting edge technologies for providing efficient security solutions by taking into the consideration of dynamic environment of MANETs. These technologies include machine learning, Artificial Intelligence (AI), Genetic Algorithms based methods, biological-inspired algorithms and so on. This paper presents a comprehensive and systematic study of various modern approaches for intensifying security in MANETs.

1. Introduction
MANET consists of mobile nodes which are connected by wireless medium in an infrastructure-less dynamic network [1]. The unique properties of MANETs increase its applications in areas where the installation of infrastructure is not feasible such as in military, rescue operations, health care, virtual conferences etc. Furthermore, in critical scenarios such as battlefield communication, security in this network is an inevitable issue. The vulnerabilities in the network make it an attractive choice for introducing attacks to breach the security. Hence, it is imperative to choose an efficient and flexible security system which should be robust enough to filter out any malicious activity from the network.

Due to dynamic nature of Mobile nodes in MANETs, the topology of the network is not fixed which poses enormous challenges in implementing any security mechanism. There is no any central authority available for communication, the network is self-configured and self-deployed [2]. Since, the communication among the nodes takes place through wireless medium; the network is more prone to errors and security threats.

In addition, each node is connected to other node in its vicinity and multi-hop communication occurs where data packets gets forwarded by many nodes in between the path. Thus, the constraints of the dynamic infrastructure in MANETs open up many areas of research in the security of MANETs [3]. The ML based algorithms can be applied in the ad-hoc environment to create a predictive model for finding out the unforeseen security threats. So, the further sections of this paper clearly specify the role of ML based algorithms in maintaining security in MANETs.
2. Security Approaches in MANETs

The unique features of MANETs such as decentralization, self-management etc. attracts various attacks in the network. In last decade, a variety of security mechanisms are proposed to detect attacks and mitigate the effects of them. The broad classification of these approaches is shown below:

The earliest security protocols in MANETs were relied upon the cryptographic approach. In 1999, a key management system for providing authentication in ad hoc networks with the help of threshold cryptography was implemented. In the proposed system, some nodes perform the task of servers and a few nodes took the role of administrator. Further, a secure version of AODV was proposed named as SAODV [4]. The proposed method implemented digital signatures and hash chains for cryptographic security in ad hoc networks. A huge number of cryptographic mechanisms were based upon the central authority for the disbursement of certificates for authentication purpose [5][6][7][8].

However, some other methods modified the concept of central supervision analogous to PGP web of trust model [9][10]. In these methods, the node itself equipped to store their certificates, thus authentication process includes a chain of certificates stored at their ends. In literature, it has been observed that the cryptographic mechanisms introduced a significant delay in the communication and a prior connection needs to be maintained between the nodes which are not feasible in ad-hoc networks. So the researchers brought together a large collection of hybrid methods for security enhancement in MANETs.

The nodes in MANETs are exposed to various kinds of attacks including active as well as passive attacks. For example, some of the common attacks are denial of service attack, man in the middle attack, flooding, spoofing, impersonation, black hole and grey hole attacks etc. In literature, various intrusion detection systems are worked to detect different type of attacks.

In nutshell, a number of cryptographic mechanisms were employed in past to introduce security features in MANETs, but in last decade, there is a shift in network paradigm as new technologies such as machine learning, deep learning, AI, genetic algorithms have become a significant choice for researchers in finding effective and optimized solutions for security in MANETs. Therefore, this paper introduces state of the art technologies which have been proved to be very effective in providing the security solutions. It involved detection, prevention, prediction and mitigation of compromised nodes and various secure routing protocols based on machine learning.

3. Security Solutions Based on Machine Learning

Security is an essential requirement for any network operations such as packets and routing protocols. While designing of sensitive applications, the critical security features of the network need to be considered. Machine Learning techniques help in designing a predictive model where model is trained with the training data for specific attack patterns and then tested by remaining test data. The accuracy of the learning model is assessed based upon the accuracy of identifying new attack patterns.

Due to open environment of the network, nodes in MANETs are more prone to different types of attacks such as black hole, worm hole, grey hole, flooding, DoS attacks etc. Furthermore, the nodes in MANETs exhibit multi hop communication which means source node passes packets to a number of intermediate nodes before destination node. Each communication depends upon the co-operation among the nodes. So, as a security measure, it is essential to figure out trustworthiness of the nodes so that packets should not be forwarded to any untrustworthy or malicious node in the network. For this purpose, there are a number of trust evaluation methods proposed in literature to enhance security in the network. Thus, security mechanisms in MANETs can be segregated into the following categories as shown in Figure 1.

Furthermore, ML plays a vital role in enhancing the security of mobile ad-hoc networks. Various ML algorithms can be suitably applied in MANETs to identify intrusions as well as specific attack patterns. Nevertheless, various trusted systems are also proposed in literature to improve security features in the network. Hence, ML based approaches for three specific areas of security in MANETs are elaborated as follows:
3.1 Machine Learning Based Intrusion Detection System

IDS (Intrusion Detection System) correspond to a defense mechanism which is deployed in MANETs to monitors and investigate suspicious events. It includes various mechanisms for identifying different kind of abnormalities in the network. In MANETs, due to open nature, the nodes can join and leave at any time which makes the network more vulnerable to different kind of attacks. The major objective of IDS is to identify any malicious activity before it can harm the network. So every node in MANETs is equipped with IDS to filter the unauthorized access. As nodes in MANETs are constrained of resources, it poses a great challenge in implementation of IDS in real life scenarios. Machine learning techniques help in identifying various novel threats and vulnerabilities. IDS can be configured based upon various machine learning techniques such as Fuzzy logic, Genetic Algorithms, Bayesian theory, neural networks.

IDS can be broadly classified into three categories, which are: anomaly detection systems, misuse detection systems and signature-based detection systems [11]. Anomaly detection systems can filter unauthorized or outlier nodes by comparing the actions of nodes with the regular normal patterns. If a node is found to behave outlier, it is labeled as intrusion. On the contrary, misuse detection systems and signature-based systems rely upon the stored signature or behavior patterns, so they are unable to detect novel attacks. Thus, anomaly detection systems outperform in terms of identifying unknown vulnerabilities as it works on the vision that any intruder never follow the regular attack pattern but the drawback is a large number of false alarms.

ML based IDSs have become a fascinating choice for researchers fraternity in order to deploy some methods which helps in reducing the true negatives and false negatives in the systems and enhancing security in MANETs. Various classification approaches in ML can be applied to classify normal and intruder nodes.

Two novel IDSs based upon hierarchical architecture and distributed architecture introduced in 2003 [12]. The proposed frameworks deployed SVM classification technique and mainly designed for securing the network layer.

Later on another classification based IDS was proposed and the authors developed a hybrid model based upon Bayesian classifier, Markov chain rules and Association rule mining for introducing security in MANETs [13]. The proposed method provided the security at different layers such as MAC, routing and application layers. The characteristics of the nodes at different layers then evaluated to identify the impostor nodes.

Further, in regard to building ensemble classifiers for IDS, a multi-level hierarchical model was introduced for collecting and processing data by using ensembles classification methodology [14]. In this, to process the anomaly indexes, clustering techniques were tested. The testing of the ensemble model was performed using two different routing protocols and using multi attack model. The authors
derived remarkable deductions regarding benefits of averaging with detection accuracy, which can improve when moving up in the node-cluster hierarchy.

The security was further enhanced by employing ANN based IDS in MANETs [15]. The model was proposed specifically for DoS type of attacks. The authors claimed that simulated model provided very high detection accuracy model, however it could perform better if less number of features selected during implementation.

A KNN based unique IDS was proposed in 2014 [16]. The model works with the Conformal Prediction K-Nearest Neighbor (CP KNN) algorithmic rule to classify the nodes based upon knowledge for anomaly detection. To reduce the classification time, non-conformity score value was exploited for multilevel repetition. The model witnessed high detection accuracy with large true positive rate and small false positive rate. The authors claimed the high confidence rate even in the presence of noisy data.

Further, a novel routing protocol independent IDS model based upon SVM classification approach was introduced [17]. The model was classified into regular and abnormal nodes with high detection rate of 94%. The authors observed that instead of mobility of nodes in the network, the system performance did not reduce and has contributed to increase the reliability of the network considerably.

Another remarkable approach of IDS based upon ANN was specified in 2019 [18]. The model implemented classification based upon ANN to identify, classify and blacklist the malicious nodes from the network. The proposed model achieved high accuracy with a detection rate of 88.23%.

3.2 Detection of Compromised or Outlier Nodes in MANETs using Machine Learning

The prime issue inherent in the functioning of MANETs is the complexity in identification and mitigation of various kinds of attacks [19]. The nodes in MANETs are quite unsecured due to open wireless nature of the network. This has stimulated several researcher’s interests into keeping their security by using latest technologies, out of which, some has been described in the previous section.

A model for detection of flooding attack using SVM classification algorithm was proposed [20]. The authors trained SVM with various attack patterns comprising flooding attack and model is tested in the simulated environment. The results show that the model can successfully identify flooding attack but cannot provide satisfactory output in case of multi-attack model. An improved attack classification model with KNN (K Nearest Neighbors) for wireless networks to classify normal and misbehaving nodes based upon their behavior patterns e.g. message forwarding rate, varying number of destination in sending messages etc was highlighted [21]. The implementation provides accurate results, however, no mechanism is provided for generating datasets. Further, a different model for classification of misbehavior nodes and normal nodes in MANETs was defined [22]. The authors applied SVM model with Ad-hoc on-demand routing protocol and the classification is performed based upon packet dropping behavior of the nodes. The performance of the approach was evaluated by calculating packet delivery ratio, packet modification and misroute ratio.

A hybrid approach consisting of SOFM (Self Organized Features Maps) and Genetic Algorithm for detection of attacks was proposed in 2018 [23]. In this, the unsupervised learning ability of the SOFM was utilized to define Neutrosophic conditional variables in MANETs. These variables and training data are given as input to the GA to analyze the fittest rules to detect different novel attack patterns. The authors claimed an accuracy of 99.3% in identification of attacks.

In addition to this, a novel approach based upon SVM classification for detection of Denial of Service Attack was illustrated [24]. The authors analyzed the model for detection of accuracy as well as computational time. Recently, a similar approach which focused on computational time to identify malicious node is adopted by the researchers [18]. They developed a model using ANN classification approach for classifying nodes into normal and blacklisted nodes. The authors designed a predictive model for identification of multiple attacks in MANETs but the accuracy obtained is 88.23% only.

In 2019, a classification of misbehavior detection into anomaly detection, intrusion detection and misuse detection was described. The authors claim that among all three methods, anomaly detection methods have the capacity to identify anonymous attacks for which system is not trained. However, an
IDS (Intrusion Detection System) can identify an event which is deviated from the regular pattern [11].

A comparison of two classification models by taking simulated network packet data as input in order to find out the efficient model for predicting various kinds of attacks in MANETs was performed [17]. The performance of both classification models which were SVM and LR analyzed based upon accuracy and detection capacity having less number of false alarms for network communication. The results showed that LR beat SVM in terms of accuracy with 100% detection accuracy and correctly identified malicious attacks in the network. LR also retained uniformity in terms of specificity, sensitivity, precision and misclassification rates. In 2020, a location-based misbehavior detection approach for providing security in MANETs was proposed [25]. In this, the authors focused on the optimized path calculation by using Learning Automata and privacy is introduced by using efficient cryptography algorithm.

3.3 Machine Learning Based Trusted System for Enhancement of Security in MANETs

The nodes in MANETs work in unreliable environment and they co-operate each other in forwarding the data packets. So, in order to secure the network, a trustworthiness value is assigned or earned by each node. Many researchers are working on these aspects of security to provide reliability in the network.

In 2004, a trust system by using K nearest neighborhood approach was presented in which the value of trust was judged based on the opinions of K trusted entities in a specified time [8]. The value of K depends upon the current state of the network as well as number of valid neighbors. However, this may sometimes lead to conflicts in the network. Due to dynamic, complex and fuzzy characteristics of trust metrics, various trust methods were defined based on fuzzy logic [26]. A global approach for evaluating trust based upon summarized trust values was provided [27]. In the defined approach, trust model relied on a defined function to calculate the degree of trust and similarly, a trust approach based on Bayesian theory was introduced by the researchers [28]. Another approach implemented reinforcement machine learning algorithm in the dynamic environment of MANETs [29]. The authors claim that the algorithm did not depend upon historical data and can predict the new node behavior in the network. And when selecting the best algorithm because of the physical distribution of MANET information, an algorithm which has the ability to be distributed among the nodes has to be chosen. Instead of considering direct and indirect trust separately, it is recommended to apply a hybrid trust approach which aggregates the trust values. Further, an enhanced trust model based upon reinforcement learning and deep learning method in MANETs was proposed [30]. The authors implemented the model using AODV protocol and classified nodes into trustworthy and untrustworthy nodes by feeding the simulated data into RNN (Recurrent Neural Network).

A trust evaluation model based on fuzzy theory was proposed in 2019 [31]. In the proposed work, three parameters were used such as Packet Drop Rate (PDR), Battery Discharge Rate (BDR) and Number of Link Requests (NLR). The proposed system provided more accuracy and less computation overhead as compared to the existing trust model on increasing the percentage of malicious nodes.

4. Conclusion

The dynamic infrastructure of MANETs poses a great challenge in introducing security in the network. To reduce the security threats, a number of security approaches are proposed in literature. As the machine learning techniques has potential of finding out unseen or unknown threats, so it has become an ardent choice among researcher’s fraternity. This paper has comprehensively categorized various ML algorithms-based security approaches in MANETs. The security approaches are divided into three dimensions such as Machine Learning Based IDS, Attack detection models and trust based models.

References

[1] Goyal N and Gaba A 2013 A new approach of location aided routing protocol using minimum bandwidth in mobile ad-
Asokan N, Ginzboorg P 2000 Key agreement in ad hoc networks
Seung Yi and Kravets R 2002 MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks
Jinarajadasa G, Rupasinghe L and Murray I 2018 A reinforcement learning approach to enhance the trust level of
Jinarajadasa G M and Liyanage S R 2019 A trust based advanced machine learning approach for mobile ad-hoc networks
Josang A and Quattrociocchi W 2009 Advanced features in Bayesian reputation systems
Buiati F, Puttini R, de Sousa R, Abbas C J B, Villalba L J G 2004 Authentication and Autoconfiguration for MANET Nodes 2004 Embedded and Ubiquitous Computing EUC 2004 Lecture Notes in Computer Science 3207 Springer.
Zhou L, Hass Z J 1999 Securing ad hoc networks IEEE Network 13 pp 24-30.
Buiati F, Puttini R, de Sousa R, Abbas C J B, Villalba L J G 2004 Authentication and Autoconfiguration for MANET Nodes 2004 Embedded and Ubiquitous Computing EUC 2004 Lecture Notes in Computer Science 3207 Springer.
Zapata M G and Asokan N 2002 Securing ad hoc routing protocols WISE ’02: Proceedings of the ACM workshop on Wireless security ACM Press.
Zhou L, Hass Z J 1999 Securing ad hoc networks IEEE Network 13 pp 24-30.
Buiati F, Puttini R, de Sousa R, Abbas C J B, Villalba L J G 2004 Authentication and Autoconfiguration for MANET Nodes 2004 Embedded and Ubiquitous Computing EUC 2004 Lecture Notes in Computer Science 3207 Springer.
Zapata M G and Asokan N 2002 Securing ad hoc routing protocols WISE ’02: Proceedings of the ACM workshop on Wireless security ACM Press.
Zhou L, Hass Z J 1999 Securing ad hoc networks IEEE Network 13 pp 24-30.