ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2021.0356

INVESTIGATION OF POTENTIAL MULTIPLE THREATS AND THEIR IMPACTS IN MANET

G. Jeeva[1] and K. Selvaraj[2]

[1]Department of Computer Science, Periyar University, India
[2]Department of Computer Science, Arignar Anna Government Arts College, India

Abstract

The dynamic nature of mobile ad-hoc network (MANET) provides consistent communication endurance. MANET is renowned for its self-configurable formation of interrelated network nodes. This decentralized property of MANET is vulnerable for various types of attacks which could impact the performance of the network and the protection of sensitive data transmitted through the network. The active node adaptation policy of MANET stipulates the possibility of multiple intruder instillations. Any intruder node can generate multiple attacks based on the potential and the rationale of the intrusion. The objective of this investigative work is to analyze the potential multiple threats and their possible consequences while using some prevailing security architectures along with relevant protocols. A common testbed is established with state-of-the-art network evaluation software OPNET in which random network environment with identical characteristics are used to evaluate the existing methods in terms of throughput, communication delays and security.

Keywords:

Mobile Adhoc Network, Threats, Internet of Things, Secure Cloud

1. INTRODUCTION

Mobile Adhoc Network (MANET) is getting widespread at a rapid pace during recent years. The improvements in digital radio technologies and the evaluation of latest generation communication systems made it possible to enjoy the geographical freedom. People tend to work from remote locations and in practical, many information technology related works can be done through the network augmentation. The operational intricacy and the exposure are increased manifold as a result of rapid increase in number of gadgets those could connect through MANET [1]. There are abundant subcategories such as Vehicular ad-hoc networks, Smartphone ad-hoc networks, Wireless mesh networks, Army tactical networks and Wireless sensor networks are emerged under the hood of MANET. Manipulating these diverged subcategories with their heterogeneous network members is a challenging task while concerning MANET functionality.

Scientist are constantly working to improve the overall user experience of MANET in terms of improving the Throughput, Packet Delivery Ratio, Security whereas reducing the End-to-End delay, IP-delay, Jitter and the Power consumption [2]. The count of battery-operated devices is also increasing swiftly in many MANET environments, in which there is an additional challenge has to be addressed to maintain the balance between power and performance. There are several research works carried out to improve the performance and to reduce the power consumption. A large number of inventions and explorations based on the above categories in which there are two possible scenarios. While trying to achieve high performance the power consumption is also increase proportional. While trying reduce the power consumption, either the performance or the security of the network is compromised. Merely a small number of projects achieved the betterment in both power and performance optimizations.

Incorporation of cloud technology connects massive number of heterogeneous nodes to a single network increases the to upgrade the overall user experience and the operational complexity of the background process is raised comparably at the same time [3].

OPNET is one of the standard simulators used in the communication network industry for establishing and upgrading modern network facilities. OPNET has an excellent combination of both graphical and programable interface [4]. This simulator is capable of projecting the outcomes of a proposed network environment by monitoring each and every activities of the member nodes along with the cumulative cluster information [5]. It has a large collection of network libraries with thousands of pre-designed node types and it also enables to include legacy user designed new node types. OPNET can handle inboard and portable network models seamlessly. This work is indented to study about the most recent research works those deal with the performance, security and power optimizations in MANET. A dedicated simulation environment is constructed in this work to measure several metrics relevant to performance and security.

2. EXISTING METHODS

As a result of aggregation and examination of a number of existing works, Internet of Things: A Secure Cloud-based MANET Mobility Model (IoTSCM) [6], A secure service discovery scheme for mobile ad hoc network using artificial deep neural network (SSDSMANET) [7], Mutual Authentication Technique with Four Biometric Entities Applying Fuzzy Neural Network in 5G Mobile Communications (MAT5G) [8], Key feature recognition algorithm of network intrusion signal based on neural network and support vector machine (KFNA) [9], Research of Security Routing Protocol for UAV Communication Network Based on AODV (SRPUAV) [10], Mobility, residual energy, and link quality aware multipath routing in MANETs with Q-learning algorithm (MRLAM) [11]. Assessment of deep learning methodology for self-organizing 5G networks (DLMS5G) [12], Efficient and secure data transmission approach in cloud-MANET-IoT integrated framework (ESDTCMI) [13], Efficient quantum-based security protocols for information sharing and data protection in 5G networks (EQSP5G) [14] and Distributed Trusted Authority-based Key Management for Beyond 5G Network Coding-enabled Mobile Small Cells (DTAKM5G) [15] approaches are referred in this work for analogy.

2.1 INTERNET OF THINGS: A SECURE CLOUD-BASED MANET MOBILITY MODEL

Internet-of-Things are ensconced throughout the smart homes and in smart cities. In IoTSCM a mobility model is proposed to interconnect IoT devices in cloud-based MANET. Hidden Markov Model is used in the two-dimensional plane for IoT smart device discovery as the first phase of IoTSCM. The framework is further designed to include the newly identified IoT smart device inside the known plane and continue the search for another IoT smart devices. By this way, all IoT smart devices are identified and aggregated into the network. A transition matrix probability is calculated to determine the gradient category of the smart devices to adapt in the MANET. The Cloud-MANET mobility model is introduced in IoTSCM to establish device-to-Device connectivity. This mobility model uses a distinct mathematical model to determine the speed and direction of a mobile IoT smart device by which the session life of a network connectivity is calculated. Amazon Cloud service is used to implement the IoTSCM Method and to show the functionality.

The mobility and performance of IoT smart devices are increased using this model which is the main advantage whereas the vulnerabilities of MANET are also persists in this work which is identified as the disadvantage of using this model.

2.2 A SECURE SERVICE DISCOVERY SCHEME FOR MOBILE AD HOC NETWORK USING ARTIFICIAL DEEP NEURAL NETWORK

An agent based cross layer security service discovery method is introduced in this work. This deep neural network intrusion detection system for MANET The software agent-based service discovery process is carried out periodically to revamp routing and security data. As per this SSDMANET model, formatting, encryption and session handling are take place in applications layer. Monitoring agent, Discovery Agent and Administrative agents are placed in the agent layer. Context management, proactive and reactive components are managed in discovery layer. Service, Quality of Service, routing and auditing are performed in data layer. Media access and stand in routing are performed in the communication layer. SSDMANET intruder detection system is implemented using JIST / SWANS.

Based on the simulation results, SSDMANET proved its higher accuracy and lower communication delays. The usage of Temporarily Order Routing and Open Shortest Path First procedures can be improved further. The periodic broadcasting process increases the data traffic congestion sometimes, which requires some optimization methods to enhance the overall performance.

2.3 MUTUAL AUTHENTICATION TECHNIQUE WITH FOUR BIOMETRIC ENTITIES APPLYING FUZZY NEURAL NETWORK IN 5G MOBILE COMMUNICATIONS

MAT5G is designed to handle two major phases of authentication. They are the Subscriber Enrolment Phase and the Subscriber Authentication Phase. These phases are involved during the subscriber login phase in WLAN, WPAN and in MANET where the authentication is performed through an access controller or through a gateway. The biometric parameters such as voice, flipping / clapping sounds and the face images are collected during the enrolment phase, the same are used for the authentication process. A database server is used to store all these biometric parameters as a backup for further verification. The database is supplied with the data source set $D_V=\{D_{VR1}, D_{VR2}, D_{VR3}\}$ in which D_{VR1} refers the most frequently used voice frequency, D_{VR2} refers the more frequently used voice frequencies and D_{VR3} refers the less frequently used voice frequencies. Similarly, $D_F=\{D_{FR1}, D_{FR2}, D_{FR3}\}$ and $D_I=\{D_{IR1}, D_{IR2}, D_{IR3}\}$ are the sets used to hold the clapping / flipping frequency ranges and face image data range. Another parameter set $D_W=\{D_{WR1}, D_{WR2}, D_{WR3}\}$ is used to administrate the frequently used salutation word of the subscriber. During the authentication phase, a fuzzy neural rule is used to measure the similarities of the pinging parameters of D_V, D_F, D_I and D_W with the corresponding datasets already in the database. The similarity index is calculated using the fuzzy neural rules which is used to provide authentication of the subscriber.

Simplicity of the mathematical calculations and the fuzzy neural rules of this method ensured the authentication speed which is the advantage of using MAT5G whereas, multiple parameter analysis increase the complexity and ambiguity of the authentication process make the authentication process vulnerable to the intruders – is the downside of this method.

2.4 KEY FEATURE RECOGNITION ALGORITHM OF NETWORK INTRUSION SIGNAL BASED ON NEURAL NETWORK AND SUPPORT VECTOR MACHINE

KFNA work combines the advantages of Neural Network and Support Vector Machine to recognize the key features of a Network Intrusion Signal. Principal Component Neural Network is used to extract the network intrusion signal characteristics and the Support Vector Machine is used to classify the normal and intruder network signals. This combination of PCNN and SVM in KFNA is used to achieve higher precision and low false positive rates. Defense Advance Research Projects Agency (DARPA) and KDD’99 datasets are used to evaluate the KFNA method.

The experiment results indicate that the precision of KNFA in identifying the DoS, Probe, U2R and R2L intruder attacks is improved to certain degrees. The future extension of KFNA work can be the computational complexity optimization in parameter selection based on a particular network.

2.5 RESEARCH OF SECURITY ROUTING PROTOCOL FOR UAV COMMUNICATION NETWORK BASED ON AODV

SRPUAV focuses on Unmanned Arial Vehicle communication. UAV network comes under the time-critical sensitive communication category. Since both the mobility and security are exhorted in UAV communication, it is a real challenge to devise a security protocol for this network category. SRPUAV work compares the performance parameters of Ad-hoc On-demand Distance Vector (AODV), Secured AODV (SAODV) and Improved SAODV (ISAODV). Several scheming aspects of AODV, SAODV and ISAODV protocols are analyzed in this work in detail. The processes of Routing discovery and routing Maintenance of ISAODV protocol is clearly analyzed in this work. The performance parameters of these protocols are measured using NS2 simulator. The overall performance comparison suggests that the ISAODV protocol gives a better performance than AODV and SAODV.

Throughput, Packet Delivery Ratio, End-to-End Delay and other communication delays are measured through NS2 gives a clear opinion about the performance of the protocols is the advantage of this work. Security- the vital parameter is not measured in the simulation which is one of the drawbacks of SRPUAV work.

2.6 MOBILITY, RESIDUAL ENERGY, AND LINK QUALITY AWARE MULTIPATH ROUTING IN MANETS WITH Q-LEARNING ALGORITHM

In MRLAM work, the authors used energy efficient nodes to frame the optimal routing path to improve the reliability, stability and lifetime. Q-Learning algorithm is used to select the intermediate nodes based on their energy level, mobility and link quality. MRLAM also concentrates in efficient energy handling and improving performance of the network. A dedicated system model is introduced in MRLAM for Energy consumption estimation of mobile nodes, Node mobility estimation and Link quality estimation of mobile nodes. MATLAB 2018a is used to simulate the MRLAM work. A number of 200 separate simulations are carried out to get best result averages. Throughput, average End-to-End delay, Packet Loss Ratio and Energy consumption are interpreted through the simulation to evaluate the performance of MRLAM. Convergence, Throughput, End-to-End delay, Packet Loss Ratio and Energy consumption are measured based on different node velocity.

The observation results show that the MRLAM method improves the performance of a network significantly which is referred as the advantage of this method. While using MANET, security is also one of the important factors that has to be taken care, which is not discussed in this work. For simulation, same configuration nodes are used to evaluate the entire model whereas a real-world MANET entity has heterogeneous nodes. Therefore, redesigning the simulation environment with heterogeneous nodes may support to improve the benchmark of this work.

2.7 ASSESSMENT OF DEEP LEARNING METHODOLOGY FOR SELF-ORGANIZING 5G NETWORKS

DLMS5G work introduced an autoencoding based machine learning framework for self-organized 5G networks such as MANET. This autoencoding based machine learning method is claimed to be more precise than conventional machine learning methods. To contrive a Deep Learning based Anomaly detection, this autoencoder is equipped with an artificial neural network architecture which comes under the unsupervised learning. The autoencoder consists two phases they are the encoder, which is used to encode the input data with bias weights and the decoder to reconstruct the input data based on the output of first phase. The simulation is performed with NS-3 Simulator with a fixed number of 105 mobile users uniformly distributed under 7 base stations. Hexagonal cell layout with 500 meters inter-site distance and a downlink full buffer network scenario is used to perform the simulations. True positive rate is analyzed for the proposed work to ensure the accuracy of the anomaly detection of DLMS5G.

The advantage of DLMS5G are better accuracy and precision. Evaluation of performance changes is one of the vital tasks should be performed while increasing the security of a network. Performance in terms of Throughput. Communication delays and Packet delivery ratio are not measured for this DLMS5G work which can be a disadvantage of this work.

2.8 EFFICIENT AND SECURE DATA TRANSMISSION APPROACH IN CLOUD-MANET-IOT INTEGRATED FRAMEWORK

Internet-of-Things, the omnipresent devices already took control over prominent portion of automations. The combination of Cloud-MANET-IoT is the rapidly growing combination by which almost all automation domains. ESDTCMI work is contributed to interlink the embedded cloud with MANET arena with improved performance and security. EDSTCMI confronted the challenges in interlinking embedded cloud with MANET such as aggregating data from billions of smart devices, optimal usage of computational resources to handle huge environment data and cutting down the data redundancy from similar kind of sensor devices.

Registration of IoT nodes with cloud servers, management of existing, lapsed and newly joined devices are the two prime tasks of ESDTCMI. The communication session life between the nodes are calculated with a consecrated formula by using node velocity. Based on this calculation, the node migration between the clusters is determined by ESDTCMI. The experimental setup is centered on Amazon Web Services (AWS) and the performance is measured based on the velocity of the nodes.

By observing the experimental results, it is understood that the ESDTCMI method provide a polish way to combine the IoT devices with cloud through MANET. This performance improvement is counted as the advantage of this work whereas the number of node variations and communication delays are not discussed – which is identified as the limitation.

2.9 EFFICIENT QUANTUM-BASED SECURITY PROTOCOLS FOR INFORMATION SHARING AND DATA PROTECTION IN 5G NETWORKS

Evolution of 5G networks improved the user experience in terms of flexibility, trust, security and privacy. It also provides enhancements in Software Defined Networks, Network Slicing and Cloud computing by providing a placid interface between numerous heterogeneous network nodes. Considering that the 5G technology is an emerging one, there are several divergences exist in the technological enhancements. The objective of EQSP5G work is to introduce an advanced cryptographic security protocol to handle the design and operational security concerns in an efficient way.

The authors of EQSP5G have introduced two major contributions in this work. They are ‘An Efficient Authenticated Key Distribution (AKD)’ and ‘An efficient Authenticated Quantum Direct Communication (AQDC)’. AKD is designed with more resistance to known security attacks during the communication between the nodes and the cloud server. AQDC is designed with a dedicated Hash Function which ensures the secured communicated between the devices, that is Device-to-Device communication. Security of EQSP5G method is analyzed against Impersonation attack, Intercept-Resend attack, Man-in-the-Middle attack, Measurement attack, Message and No Message attacks. Computed Hash values are analyzed using confusion distribution, diffusion distribution and uniform distributions.

The security analysis is produced as proof-of-concept approach may vary due to real-world dynamic network environments. The analysis are performed based on some initial assumptions which may not be appropriate always to the real network environment. The influence of the EQSP5G method on the performance of the network in not discussed in this method, which requires further study through benchmark network simulators.

3. DISTRIBUTED TRUST AUTHORITY-BASED KEY MANAGEMENT FOR BEYOND 5G NETWORK CODING-ENABLED MOBILE SMALL CELLS (DTAKM5G)

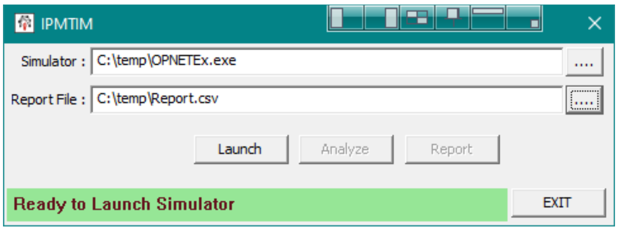
DTAKM5G work discussed about the preamble of Network Coding-enabled Mobile Small Cells (NC-MSC). This technology makes it possible to establish dynamic network setup on-the-go. NC-MSC is also permits the multi-hop device-to-device communication for paramount network offloading. The core of DTAKM5G is the decentralized key management security scheme that provides threshold secret sharing based certificate authority function distributions. An individual Anywhere-Anytime standard master private key for every node to intensify the flexibility of the network. Network Initialization, Management of self-generated Certificates, Verification of self-generated certificates, Secure communication establishment, Node adoption and Proportional updating are the phases are addressed properly in this DTAKM5G work.

The security issues and enhancements are discussed theoretically. The performance amendments during the application of DTAKM5G are not discussed in this work. Implementation or simulation of the proposed model is not put forward as well. A complete analysis of the impact on security and performance of the 5G network during the utilization of DTAKM5G method has to be realized by performing a touchstone simulation is required to demonstrate the benefits and constraints of this work. A table is provided below to expound the procedures, advantages and the limitations of the above discussed existing methods.

4. EXPERIMENTAL SETUP

A unified experimental setup is applied here to evaluate the performance of the selected methods. OPNET is utilized here to simulate the discussed methodologies in terms of Throughput, End-to-End Delay, Packet Delivery Ratio and Security. Even though the discussed methods are all deals with MANET, the applications of these methods are moderately deviated. A shared network environment with 5000 m^2 with heterogeneous MANET nodes is taken in this simulation to meet the analytical requirements for the methods. The nodes are placed in a uniformly distributed random placement pattern. The traffic is also initiated as typical random traffic with control data, text data, voice and streaming data to replicate the real-world scenario. OPNET has a wonderful stipulation to integrate the Graphical User Interface with programming scripts [16]. OPNET is also equipped with a great deal of built-in libraries, node types, network components, protocols and to load the user defined network components and architectures [17]. The facility to load and run C++ programs works seamlessly which is one of the cutting-edge architectures available in OPNET. It has the facility to analyze the security by generating a sequence of attacks into the simulating environment.

Visual Studio is used to design a dialog-based user interface to access the OPNET simulator. The network protocols and communication concepts are scripted in VC++ language and supplied to OPNET for loading the user defined methods [18] [19]. The simulation is performed for 24 hours of real-world time to measure the evaluation metrics of the methods. The user interface is given in Fig.1. A typical node placement in OPNET is given in Fig.2.


IPMTIM

Simulator : C:\temp\OPNETEx.exe

Report File : C:\temp\Report.csv

Ready to Launch Simulator

Fig.1. User Interface

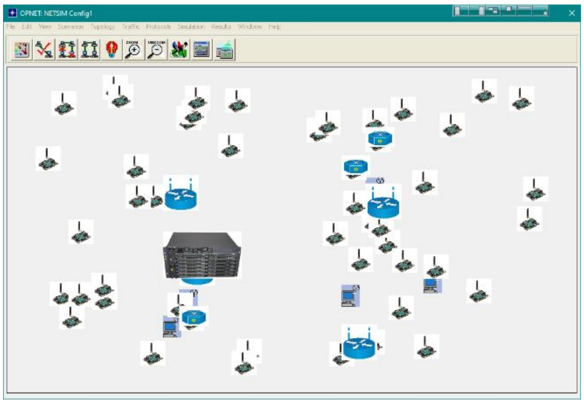


Fig.2. OPNET Node placement

5. RESULTS AND ANALYSIS

Simulation is performed for 24 hours real-world time with 100 to 1000 nodes in step 100. The simulation begins with 100 number of nodes and for every 2 hours and 24 minutes, 100 nodes will be increased gradually. Therefore, at the end of 24 hours simulation, the total number of nodes will be 1000.

For every 2 hours and 24 minutes, parameters such as Throughput, End-to-End delay, Packet Delivery Ratio and Security are measured by OPNET and logged to the report. After completion of the entire simulation, the report is exported as an Excel sheet for further analysis. The tables and graphs are provided in this section in detail.

5.1 THROUGHPUT

Throughput is a measurement of data transferred through a particular channel during a standard time period. In general, the higher value of throughput refers the higher performance of the network architecture. It is also notable that a good communication protocol can improve the performance of the network by increasing the throughput. Measured throughput values are given in Table.2.

As per the simulation results, MAT5G and SRPUAV methods achieved highest throughput value of 29358 kbps. MAT5G achieved the highest throughput during the initial stage of the simulation whereas, SRPUAV achieved the same value during the simulation phase with 200 nodes.

It is also observed that the throughput values are decreasing gradually based on the increased node count. Based on the throughput value average, the performance-wise sequence is MAT5G, SRPUAV and ESDTCMI got the first three places given in order. DLMS5G got the least throughput average value of 22858.8 kbps.

5.2 END-TO-END DELAY

End-to-end Delay is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counts. The lesser values of End-to-End delay shows the higher quality and performance of the network. The measured End-to-End delay values are tabulated below in Table.3.

Based on the observation, MAT5G has the lowest End-to-End delay average value 318.9 mS. The successive performers are SRPUAV and ESDTCMI with the End-to-End delay averages 340.1 mS and 368.4 mS respectively.

5.3 PACKET DELIVERY RATIO

Packet Delivery Ratio (PDR) is the calculation of proportion between the number of packets received in the destination and the number of packets transmitted from the source. The PDR value is directly proportional to the performance of the network. That is, the higher values of PDR indicate the higher performance of the network. Calculated PDR values during the simulation are given below in Table 4.

According to the simulation results, the highest PDR 94% is achieved by SRPUAV. The PDR average of SRPUAV method is 90.1%. The consecutive methods in PDR average are MRLAM and IoTSCM both with the value of 88.1%.

5.4 SECURITY

Security in one of the primary parameters while considering any mode of private communication. Security is measured in percentage units which is determined by the ratio between number of packets attacked with several intruder attacks and number of compromised packets.

A good security protocol should give better security levels. The simulation results of security analysis are given below in Table.5.

Table.1. Advantages and limitations of existing methods

Work	Methodology	Advantages	Confines
IoTSCM [6]	HMM Transition Matrix Probability	Mobility and Performance	Inherited MANET security issues
SSDSMANET [7]	Agent based cross layer Deep Neural Network	Security	Data Congestion
MAT5G [8]	Biometric parameter-based authentication	Authentication Speed	Security
KFNA [9]	Integration of Neural Network and SVM	Security	Computational Complexity
SRPUAV [10]	Secure AODV	Performance	Security
MRLAM [11]	Q-Learning Algorithm	Performance	Node type restriction
DLMS5G [12]	Auto-Encoding based Machine Learning	Security	Performance
ESDTCMI [13]	Embedded Cloud Security	Performance	Node count limitation
EQSP5G [14]	AKD and AQDC	Security	Performance
DTAKM5G [15]	NC-MSC	Security	Performance

Table.2. Throughput (kbps)

Nodes	IoTSCM	SSDSMANET	MAT5G	KFNA	SRPUAV	MRLAM	DLMS5G	ESDTCMI	EQSP5G	DTAKM5G
100	28310	27067	29358	27803	29201	28759	26655	28858	28277	28678
200	28559	26819	29217	28254	29358	29031	26680	29155	28344	28720
300	26484	24841	27223	25893	27032	26851	24913	27095	26399	26655
400	26238	24804	27140	26084	27297	27033	24972	26877	26361	26954
500	24431	23065	25177	24266	25450	24871	22875	24970	24449	24787
600	24439	22933	25531	24154	25182	24873	23095	24997	24285	24661
700	22376	21196	23264	22264	23252	23155	20743	22969	22419	22650
800	22597	21074	23446	22276	23254	22820	20708	22911	22425	22833

900	20303	19187	21614	19962	21374	21230	19019	21012	20485	20747
1000	20355	18817	21483	20022	21442	20944	18928	21158	20135	20877

Table.3. End-to-End Delay

Nodes	IoTSCM	SSDSMANET	MAT5G	KFNA	SRPUAV	MRLAM	DLMS5G	ESDTCMI	EQSP5G	DTAKM5G
100	386	413	304	401	330	362	423	353	400	383
200	392	423	311	401	331	360	429	357	402	379
300	393	419	308	409	332	368	429	361	409	382
400	394	428	313	414	339	366	435	362	413	389
500	403	426	318	412	343	374	436	369	413	392
600	398	430	323	415	338	375	433	370	414	393
700	400	436	320	420	345	377	441	372	416	397
800	412	439	325	427	343	381	441	378	428	404
900	411	442	331	422	346	383	443	382	425	399
1000	415	440	336	434	354	389	453	380	430	403

Table.4. Security (%)

Nodes	IoTSCM	SSDSMANET	MAT5G	KFNA	SRPUAV	MRLAM	DLMS5G	ESDTCMI	EQSP5G	DTAKM5G
100	93	90	90	91	94	92	91	91	91	93
200	92	89	90	90	93	92	91	90	91	91
300	90	88	89	89	93	90	89	89	89	90
400	90	87	88	89	92	90	89	89	89	90
500	88	87	86	88	91	89	87	87	87	89
600	87	86	86	86	89	87	87	87	86	88
700	87	85	84	85	88	87	85	86	85	86
800	85	84	84	84	88	85	85	85	85	85
900	85	83	83	83	87	85	83	83	84	84
1000	84	82	82	82	86	84	83	83	82	84

Table.5. Security (%)

Nodes	IoTSCM	SSDSMANET	MAT5G	KFNA	SRPUAV	MRLAM	DLMS5G	ESDTCMI	EQSP5G	DTAKM5G
100	89	93	91	94	95	89	94	88	94	95
200	88	92	91	94	95	88	94	88	95	94
300	88	92	92	94	95	89	93	88	94	95
400	89	92	92	94	95	89	94	87	95	94
500	89	92	91	94	95	88	93	88	95	94
600	88	92	92	93	94	89	93	87	94	94
700	88	92	91	93	95	89	93	88	95	95
800	88	93	91	93	94	88	93	88	95	94
900	89	92	91	94	94	89	94	88	94	94
1000	88	92	92	94	95	88	94	88	95	94

Highest security average is achieved by SRPUAV with the value 94.7%. The ensuing methods based on security average values are EQSP5G and DTAKM5G in order with the values 94.6% and 94.3% respectively.

6. CONCLUSION

A set of MANET security proceedings are studied in this work to understand the functionality against multiple threats and their impact on the performance. Based on the studies, it is understood that the high-performance protocols are lacking security whereas the protocols with higher security influence the performance. According to the simulation results, one of the existing methods MAT5G scores high in terms of throughput which is in the first position, got the 7th place in terms of security. Based on the analysis, it is understood that, even though there are plenty of network models and protocols available for MANET, it is necessary to carryover new research works in this field to develop a performance-security balanced working model to improve both performance and security simultaneously.

REFERENCES

[1] Tanweer Alam, "Device-to-Device Communications in Cloud, MANET and Internet of Things Integrated Architecture", *Journal of Information Systems Engineering and Business Intelligence*, Vol. 6, No. 1, pp. 18-26, 2020.

[2] K.M. Balamurugan and S.V. Bhanu, "A Multi-Objective Krill Herd Algorithm for Virtual Machine Placement in Cloud Computing", *Journal of Supercomputing*, Vol. 76, No. 6, pp. 4525-4542, 2020.

[3] M. Krzyszton and E. Niewiadomska Szynkiewicz, "Adaptation of MANET Topology to Monitor Dynamic Phenomena Clouds", *Proceedings of International Conference on Computer Science and Information Systems*, pp. 865-872, 2017.

[4] M. Pahlevan and R. Obermaisser, "Evaluation of Time-Triggered Traffic in Time-Sensitive Networks using the OPNET Simulation Framework", *Proceedings of International Conference on Parallel, Distributed and Network-based Processing*, pp. 283-287, 2018.

[5] S. Lee, J. Ali and B. Roh, "Performance Comparison of Software Defined Networking Simulators for Tactical Network: Mininet vs. OPNET", *Proceedings of International Conference on Computing, Networking and Communications*, pp. 197-202, 2019.

[6] Tanweer Alam, "Internet of Things: A Secure Cloud-Based MANET Mobility Model", *International Journal of Network Security*, Vol. 22, No. 3, pp. 1-17, 2020.

[7] N. Islam, "A Secure Service Discovery Scheme for Mobile Ad Hoc Network using Artificial Deep Neural Network", *Proceedings of International Conference on Frontiers of Information Technology*, pp. 133-1335, 2019.

[8] Pijush Kanti Bhattacharjee, "Mutual Authentication Technique with Four Biometric Entities Applying Fuzzy Neural Network in 5G Mobile Communications", *IOSR Journal of Electronics and Communication Engineering*, Vol. 15, No. 3, pp. 38-46, 2020.

[9] Kai Ye, "Key Feature Recognition Algorithm of Network Intrusion Signal Based on Neural Network and Support Vector Machine", *Symmetry*, Vol. 11, No. 3, pp. 380-395, 2019.

[10] Xiaopeng Tan, Zhen Zuo, Shaojing Su, Xiaojun Guo and Xiaoyong Sun, "Research of Security Routing Protocol for UAV Communication Network Based on AODV", *Electronics*, Vol. 9, No. 8, pp. 1185-1195, 2020.

[11] Valmik Tilwari, Kaharudin Dimyati, M.H.D. Nour Hindia, Anas Fattouh and Iraj Sadegh Amiri, "Mobility, Residual Energy, and Link Quality Aware Multipath Routing in MANETs with Q-learning Algorithm", *Applied Sciences*, Vol. 9, No. 8, pp. 1582-1598, 2019.

[12] Muhammad Zeeshan Asghar, Mudassar Abbas, Khaula Zeeshan, Pyry Kotilainen and Timo Hamalainen, "Assessment of Deep Learning Methodology for Self-Organizing 5G Networks", *Applied Sciences*, Vol. 9, No. 15, pp. 2975-2989, 2019.

[13] Tanweer Alam, "Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT Integrated Framework", *Journal of Telecommunication, Electronic and Computer Engineering*, Vol 12, No. 1, pp. 1-13, 2020.

[14] Ahmed A. Abd EL-Latif, Bassem Abd-El-Atty, Salvador E. Venegas-Andraca and Wojciech Mazurczyk, "Efficient Quantum-based Security Protocols for Information Sharing and Data Protection in 5G Networks", *Future Generation Computer Systems*, Vol. 100, No. 1, pp. 893-906, 2019.

[15] M. De Ree, G. Mantas, J. Rodriguez and I.E. Otung, "Distributed Trusted Authority-based Key Management for Beyond 5G Network Coding-enabled Mobile Small Cells", *Proceedings of International Conference on 5G World Forum*, pp. 80-85, 2019.

[16] Zheng Lu and Hongji Yang, "*Unlocking the Power of OPNET Modeler*", Cambridge University Press, 2019.

[17] Maryam Pahlevan and Roman Obermaisser, "Evaluation of Time-Triggered Traffic in Time-Sensitive Networks using the OPNET Simulation Framework", *Proceedings of International Conference on Parallel, Distributed and Network-based Processing*, pp. 283-287, 2018.

[18] David Basin, Cas Cremers and Catherine Meadows, "*Model Checking Security Protocols*", Springer, 2018.

[19] Sun-Ju Kim, Ji-Hyun Min and Han-Na Kim, "The Development of an IoT-Based Educational Simulator for Dental Radiography", *Proceedings of International Conference on Healthcare Information Technology for the Extreme and Remote Environments*, pp. 12476-12483, 2019.