Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 7, No. 2, August 2019, pp.843-852
Available online at: http://pen.ius.edu.ba

Reactive protocols for unified user profiling for anomaly detection in mobile Ad Hoc networks

Nariman Jabbar Qasim[1], Saja Majeed Mohammed[2,] Ali Sami Sosa[3], Israa Al_Barazanchi[4]
[1]Civil Eng. Dept, Al Esraa university college
[2]Information and Communication Engineering Department, Al Khwarizmi Engineering College, University of Baghdad
[3]Computer Science Department, College of Science, University of Baghdad
[4] Baghdad College of Economic Sciences University - Baghdad, Iraq

Article Info

Received Jan 12, 2019

Keyword:

First keyword
User Profiling
Anomaly Detection
KPI
Cellular Communication
Traffic
MANET

ABSTRACT

The Next Generation mobile network expected to be fully automated to meet the growing need for data rates and quality in communication. These prodigious demands have also increased the amount of data being handled in these wireless networks. The cellular networks can leverage vital data about the user and the network conditions providing all-inclusive visibility and intelligence in communication. Emerging analytic technologies such as big data and neural networks have been used to unearth vital insight from network traffic to assist intelligent models in routing packets. Reactive protocols are an emerging model in the intelligent routing of traffic in ad-hoc networks. In this paper, we first utilize the reactive protocols to route traffic in a wireless network while analyzing anomalous behavior. In the case of anomaly detection in wireless communication, combined performance indicators to identify outliers. The detected outliers been compared with the ground data and routes created using the reactive protocols. The combination of reactive protocols and the key performance indicators in network performance uncovered anomalies leading to segregation of these traffic in routing. From the results, it is evident that an abrupt surge in the traffic indicated an anomaly and identify the areas of interest in a network especially for resource and path allocation and fault avoidance. A MATLAB GUI was used to simulate the reactive protocols for routing of traffic and generation of datasets that analyze in Microsoft Excel to characterize the key performance indicators of the network.

Corresponding Author:

Israa Al_Barazanchi[4],
Computer science department,
Baghdad College of Economic Sciences University,
Baghdad, Iraq https://orcid.org/0000-0002-6798-6295
Email: Israa44444@gmail.com.

1. Introduction

The continuous growth in mobile technology leading to faster data rates and the increase in sensitive information has led to most service in base stations to be targets of malicious attacks. Recently, ad-hoc networks have become targets of attack due to the increased client-server inquiry. The services are typically accessible via numerous ports that can be open via the firewalls. New network architectures like 5G enhance multimedia communication availing this technology at the user’s disposal [1]. The primary concern of these cellular networks is security. The increased complexity of this network has also made the task of detecting preventing and repulsing abuse. In communication, it's not guaranteed that any system can be made secure, but the recent techniques in security such as authentication of users and encryption have improved the monitoring of cellular network guaranteeing a level of security [2]. The need for user profiling and authentication is based on the fact that most attacks on cellular networks are based on software flaws and design errors that can be easily combined to provide a malicious door to the system, for instance, the recent cloning of GSM cards [3]. These incidents have made it vital to develop countermeasures such as they normally detection that is reliant on the profiling of the network users. The anomaly detection is the process of identifying outliers or abnormal incidences in any communication system for instance behavior that is substantially different from the normal network traffic.

The cellular networks are typically distributed to allow for reuse of transmission frequencies. In cellular networks, the local database (VLR) and mobile switching center (MSC) are distributed to serve localized regions which are divided into local areas (LA) that are further divided into cells [4]. The cell is reachable to any network user due to the mobility of cellular networks. This mobility in wireless communication networks makes it vital that the user's location information is managed. The management of this information takes into rumination the performance of the network with regards of the local area (LA). In mobile networks, the management of user location and other communications are organized in a central database known as the home location register (HLR) [5]. The HLR stores all the subscribers’ information and the base station therefore anytime a user enters a new LA they are transferred to a new MSC which allows for the downloading of only the pertinent information to the VLR . In case a mobile terminated call is made from a switched telephone network such as PSTN then this communication will be routed via a gateway, i.e., gateway MSC. The gateway MSC (GMSC) will interrogate this connection which will be forwarded to the HLR. The HLR will query the relevant VLR which will analyze and determine the routing number for the visited MSC. The MSC will initiate a paging message that will be sent to the relevant Base Station (BS) which will broadcast the message through all cell to the user equipment (UE). This process of location update (LUP) and paging are the fundamental tasks accomplished in tracking and locating a user. The two processes are carried out in granularity; thus, mobile networks have the foundational task of locating a user [5]. This information makes it easy to define user mobility and behavior patterns; therefore, any changes can easily be tracked as an anomaly and corrected.

In this study, we will focus on reactive protocols to generate user traffic for anomaly detection in a mobile network. Outlier detection in mobile networks has specific user characteristic and security requirements. Therefore, we introduce a new model that is based on reactive protocols for routing and critical performance indicators for the detection of anomalies in network traffic.

Study contribution: This paper contributed the study in three different ways. First, provided a detailed background on the existing techniques and methods used for normally detection in various networks such as web-based application and VANETs. Secondly, evaluate the related work in user profiling which been vital in the collection of the essential features during the simulation in MATLAB. Third, simulated the user traffic using a MATLAB GUI to obtain the necessary data set for principal performance indicators analysis to detect the outlier in the network.

2. Related work

Most works of literature have shown that anomaly detection has already been performed using learning techniques either supervised or unsupervised, statistical methods, stream analytic engine and data-mining approaches [6]. Little has been done with regards to reactive protocols used in ad hoc network and key performance indicators to detect outliers in a network. These two proposed techniques considered a massive dataset to mimic the current situation of an increased number of users in mobile networks [4]. This section evaluated the relevant knowledge with regards to reactive protocols, user profiling, and anomaly detection. The knowledge that been created form a foundation for the simulation of that scenario presented.

2.1 Reactive Protocols

Mobile ad-hoc networks (MANETs) describe temporary cellular networks that are made of mobile nodes which utilize a similar randomaccess wireless channel in which the mobile nodes act as the hosts and routers [1,7]. Examples of MANETs are vehicular ad hoc networks (VANET), intelligent vehicular ad-hoc networks

(InVANETs) and Internet-based mobile ad-hoc networks (iMANETs). In MANETs, various routing schemes such as the reactive and proactive which conventionally compete for unicast, multicast and broadcast communications [8]. Each routing protocol has its unique characteristic and benefits, but in this case, dwell on the reactive routing protocol. The reactive routing protocol is an approach that seeks to create a route on demand for instance if a network point wishes to commence conveyance with another point to which it has no paths then this routing convention try to initiate a route. The reactive routing protocols maintain the routing data in all the confluence in the network every time. This task is event-driven and is characterized by low route setup latency. The four types of reactive routing protocols i.e., Ad-hoc on-demand distance vector routing (AODV), temporary ordered routing protocol (TORA), dynamic source routing (DSR) and location-aided routing (LAR) [2,4].

2.1.1 Ad-hoc on-demand distance vector routing (AODV)

This protocol employs the DSDV algorithm which traditionally minimizes the quantity of broadcasts required to create a route on demand. This protocol is contrary to maintaining an entire list of routing data at the nodes, therefore, reducing the system requirements to broadcast in extremities. The protocol does not keep the routes to neighboring node, but rather they are discovered and maintained when needed. The network points that are not included in a chosen path do not contain any routing data therefore when an origin node wants to transmit information to a target point which it does not previously have the plausible route [2,9]. This node commences path discovery by generating a route request (RREQ) to locate the new node and broadcast the route to its neighbors until the destination node is located as illustrated in figure 1. AODV employs the destination sequence data to determine that all the pathways are loop-free, and the network points contain the most updated routing data [2]. The discovered route between the origin and the terminus nodes is preserved if it is required for communication by the source. In this study, we applyed the AODV technique for communication between the source and the destination nodes.

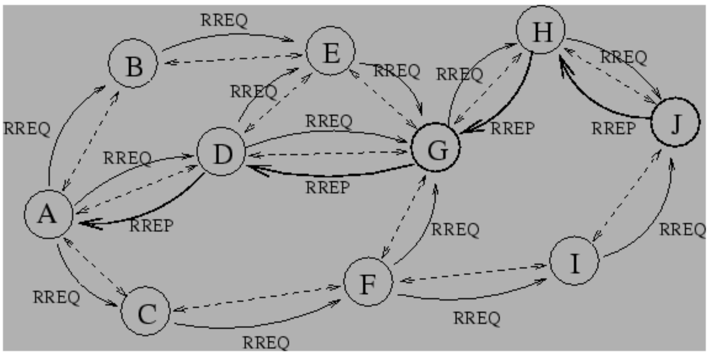


Figure 1: Possible routes from source A to J using AODV

2.1.2 Temporary ordered routing protocol (TORA)

This protocol aims at attaining a high level of scalability in utilizing non-hierarchical routing algorithm. This algorithm tries to subdue the production of far-reaching monitoring message propagation [2,3]. TORA does not utilize the shortest path selection technique but rather uses the localization of control message to minute sets of nodes. The nodes maintain the routing information for a single hop, i.e., adjacent nodes. The primary use of this approach is for route creation, maintenance, and erasure [9].

2.1.3 Dynamic source routing (DSR)

This is an on-demand routing approach in which the path is only discovered after the source point has sent a packet to the target node. Initially, the origin node has no way to the destination; thus, the mobile nodes are expected to maintain a cache of the known that the source utilizes to transmit information. The route cache is consistently updated to store the complete list of the IP addresses of which device located on the path to the terminal node. When the path from the source to the target does not exist a route request packet is broadcasted via the ad hoc network. The intermediate nodes only broadcast the packet of the appending their IP addresses to the list on the request package. Ultimately, the final node received the packet with an updated path from the origin and sends a reply packet that contained the entire path from the source to the target [2,9]. In the maintenance of the chosen route, each node in the path is responsible for the validity of the downstream link between itself and the next hop, especially in the source route.

2.1.4 Location-aided routing (LAR)

This routing protocol utilizes the flooding algorithm with the location data of a specific node limiting flooding in the network. The location information is collected via numerous positioning techniques such as GPS where the LAR computed the expected zone of a specific node. The expected zone is the location of a moving node at a given instant in time. The LAR limits flooding in any network using the requested zone, i.e., a node only transmits a packet if it's their requested zone and discarded if it's not [9]. In determining the identity of the requested zone, the LAR computed the coordinates of the requested zone [15-17]. Table1 below illustrates the three primary reactive protocols and their areas of applications.

Table 1. The Reactive protocols

Reactive Protocols	**Functionality**	**Application**
DSR	No periodic messages without reaction to the current unconcerned changes	Multi-hop wireless Ad-Hoc networks
AODV	Used by mobile nodes in Ad-hoc networks	Mobile Ad-Hoc Networks
TORA	Multiple loo-free path for communication	Wireless mesh networks

2.2 User profiling

User profiling has become a crucial component of network security especially in anomaly detection and access control. The user profiling in this research has been vital assisted in creating a benchmark for the traffic behavior in mobile ad-hoc networks making it easy to detect anomalies. In this section, reviewer a few standard models used in user profiling.

According to Pannell and Ashman [10], an intrusion detection system was utilized to monitor a user's browser history and Windows OS audit logs. In this model, a different type of users' profile created such as profiles based on websites viewed, profiles based on applications utilized, application performance and requirements, etc. These profiles were used to monitor the users' behaviors and data so that anomalies can be detected based on access to unauthorized data with regards to the profile. Furthermore, comparative data was generated from authorized access to information with regards to a single behavior profile of each user. The limitation of this model was based on the impact of the single behavior profile when applied to unauthorized data accessed by combined profiles. This model also did not apply other user behaviors such as social network activities.

Grˇcar, Mladeniˇc, and Grobelnik [11] proposed a new system for user profiling which was implemented as a toolbar in Internet Explorer (IE). In this approach, the authors maintained the user profiles as interest-aimed topic ontology. Each topic ontology was related to a collection of users viewed web pages. The authors discovered that the web pages were related to a specific topic through the analysis of the viewed content. Considering that the user profiles were created based on these viewed web pages this tool could easily be used as a guide for users to navigate to the interested webpages. The primary challenge for this tool was that it could only recommend visited web pages; therefore, further research is recommended to create a system that can recommend a user best on potentially interesting content.

Ortigosa [12], designed a Facebook application that could anticipate a user personality in the Social platform. The predictions were made based on the user's profiles as presented on Facebook. These profiles describe the user interaction with the Facebook platform such as the number of posts, number of friends and the posts written by friends. The user profile was constructed based on the hypothesis that uses with a similar personality would exude the same behavior pattern. This proposed system was limited by the fact that

Facebook is a single platform among numerous social media sites such as Twitter, Instagram; therefore, it is not easy to characterize a user's as surfing behavior.

Corney [13] utilized a computer system log to define user profiles in their research. A user profile was created based on the patterns recorded in running programs and processes in a computer system. Instances that deviate from the traditional user behavior would trigger an alert that would notify the administrator as an anomaly. They applied a grouping technique for the applications to eliminate the chances of false positive alerts. This approach was based only on computer systems; thus, it was restrictive to a user's behavior especially online.

The table 2 below illustrates the comprehensive results of the user profiling analysis. The features presented in the table illustrate why the reactive protocols is a vital technique in user profiling, especially in MANETS. The reactive protocol allow communication between the source and the destination node.

Table 2. The user profiling techniques

#	**Profiling Technique**	**Data extracted**	**Advantages**	**Disadvantages**
1	Statistical Model	Logs	-Profile users based on browser history and system use	-Does not considered hosted-based anomaly
2	Statistical Model	Logs	-Profiling using topic ontology	-Does not consider user interest on unviewed pages
3	Machine Learning	Facebook data	-Profiling user interactions in Facebook	-Limited to Facebook
4	Statistical Model	Logs	-Computer system user profiling	-Reliant on system logs

2.3 Anomaly detection

The anomaly detection procedure in this research utilizes a numerical quantification of the deviations from the characteristic routing in the network [18-20]. The defined profiles provided the benchmark for the normal behaviors of the network nodes. Therefore, the anomaly has been defined using a KPI technique illustrated belong.

$$\alpha(t) = \frac{X(t) - \mu_t}{\sigma_t}$$

Where

$X(t)$ is the initial KPI value in the time instance t
μ_t is the mean at the time instance t
σ_t is the standard deviation at the time instance t

The KPI method is used to normalize the data where the average of the anomalies been set at zero where is the standard deviation would been give the value one. This technique maked the comparison of the results using KPI easy as the normalization data in multi-dimensional cases such as in MANET with only one parameter supplied such as the routing information [21]. This normalization eliminated the fact that one dimension may suppress the impact of other measurements due to the difference in magnitude. The standard deviation of the data collected will be utilized in detecting outlier.

3. Methodology

In this study three steps were utilized for the detection of anomalies in the MANETs; the route discovery using the AODV algorithm, dataset, and KPI analysis and the implementation of the system in MATLAB

3.1 Routing of the packets

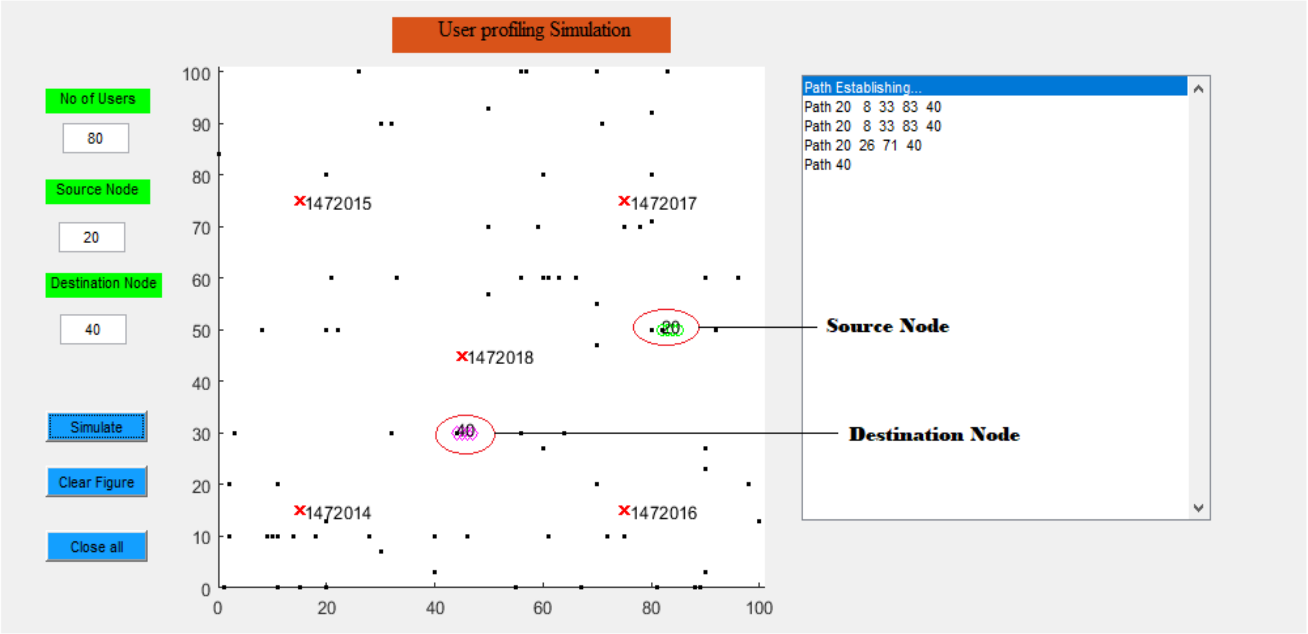
In route discovery for communication, the source point will commence path discovery by generating a route request (RREQ) to locate the new node and broadcast the route to its neighbors until the destination node is located [2]. AODV employs the destination sequence data to determine that all the roots are loop-free and the nodes contain the most current routing data. The discovered path between the origin point and the destination nodes is preserved if it's needed for communication by the source. In this research, the AODV routing protocol was applied in the MATLAB simulation for communication between the source and the destination nodes.

3.2 Dataset and KPI

The dataset that was used for the computation of the KPI was generated through the MATLAB simulation by defining the number of users, the quantity of source points and the point of destination nodes [2]. The dataset generated will then be applied in a computational equation to determine the key performance indicators. The KPI method is used to normalize the data where the mean of the traffic changes is set at zero where is the standard deviation would be specified at one. This technique will make the comparison of the results using KPI easy as the normalization data in multi-dimensional cases such as in MANET with only one parameter supplied such as the routing information. This normalization will eliminate the fact that one dimension may subdue the impact of other measurements due to the difference in magnitude. The standard deviation of the information collected will be utilized in detecting outlier.

3.3 Implementation

The AODV protocol was implemented using a GUI in MATLAB. The GUI will allow the specification of the number of users and the paths from the origin node to the target node. Figure 2 below illustrates the GUI used for the routing and path discovery in a MANETs.



```
Path Establishing...
Path 20   8  33  83  40
Path 20   8  33  83  40
Path 20  26  71  40
Path 40
```

Figure 2. The GUI used to take input and describe the various paths that can be taken from the source node to the target node

4. Results and observation

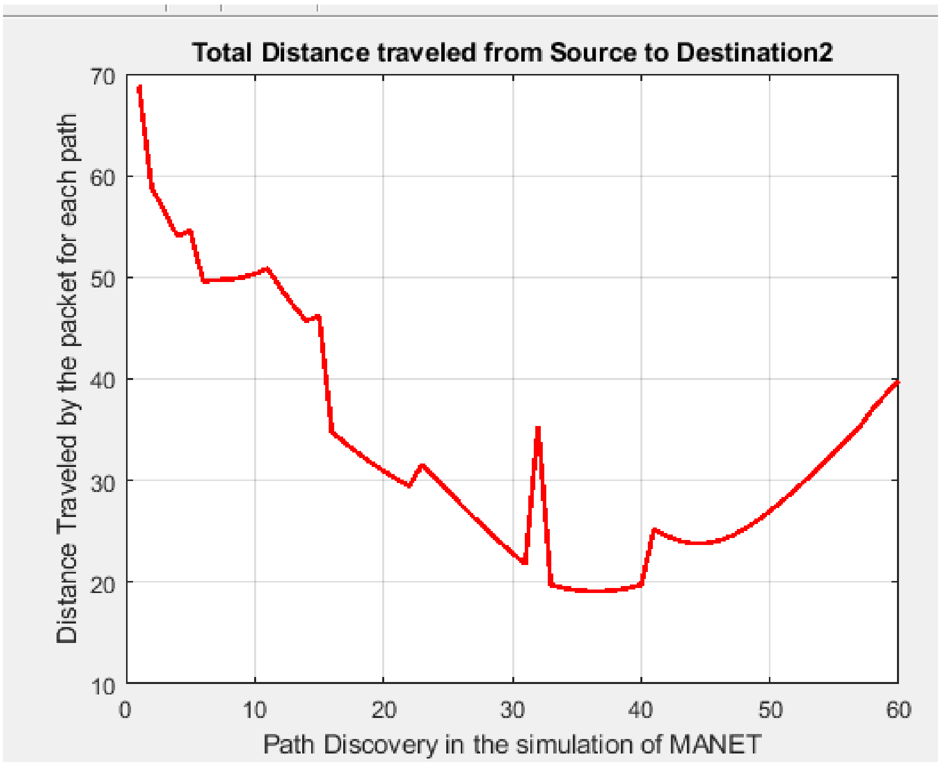


Figure 3. The Total distance traveled showing the anomaly as the packet seeks for the path from source to the target.

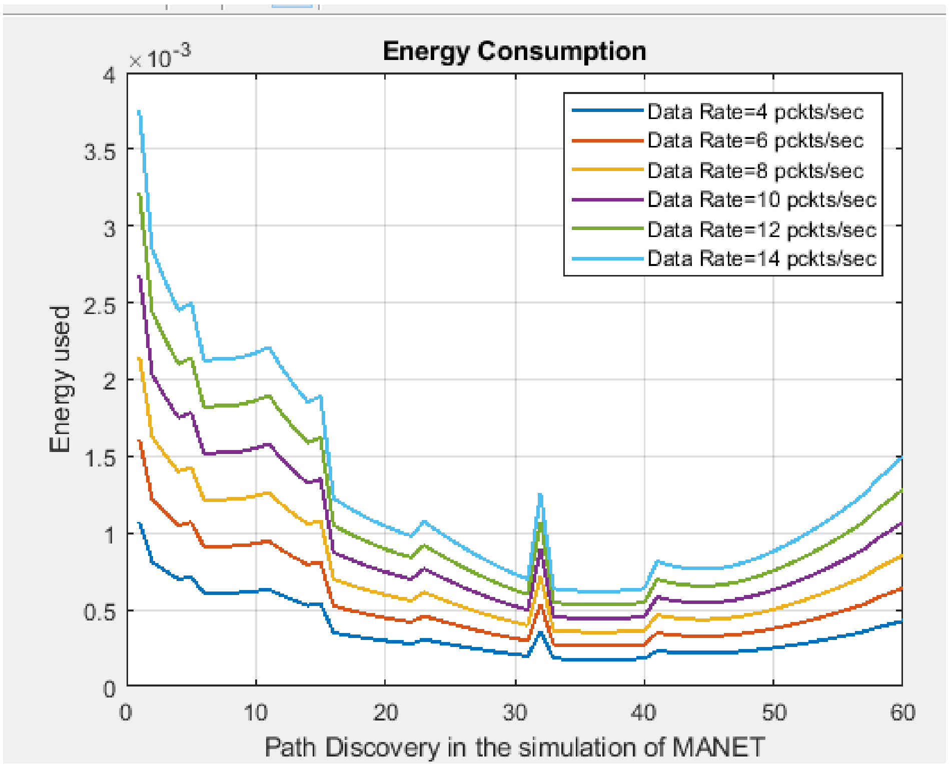


Figure 4. Results for outlier detection in energy consumption in the network for various data rates

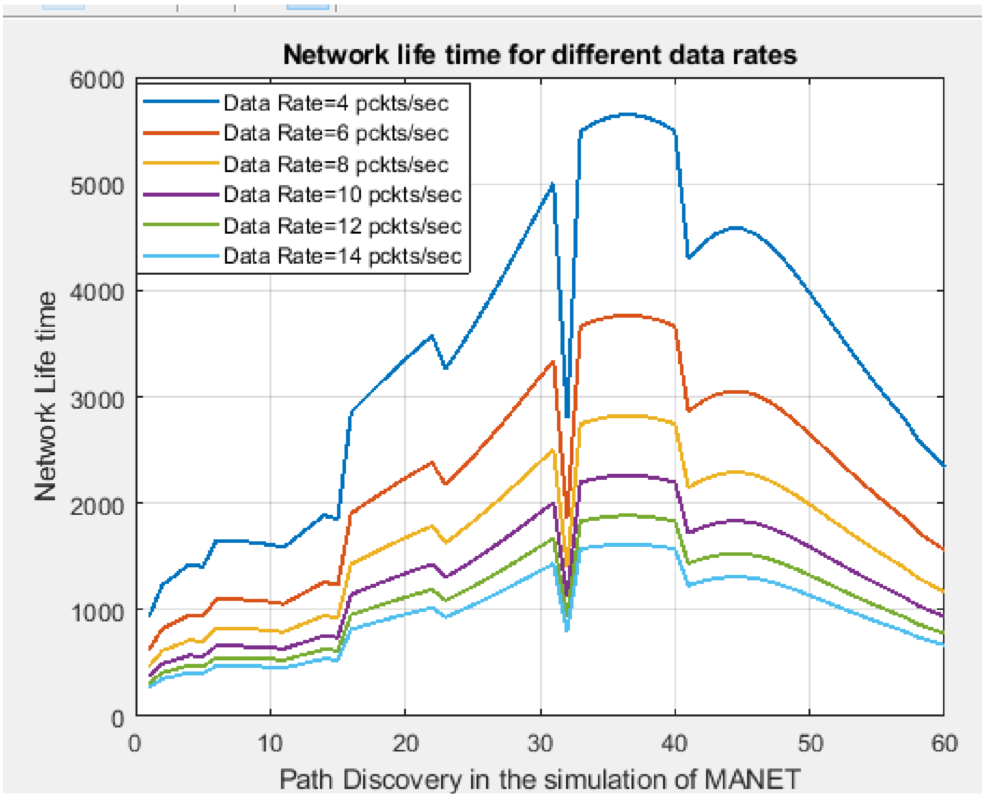


Figure 5. Results for anomaly detection in the network lifetime for distinct data rates

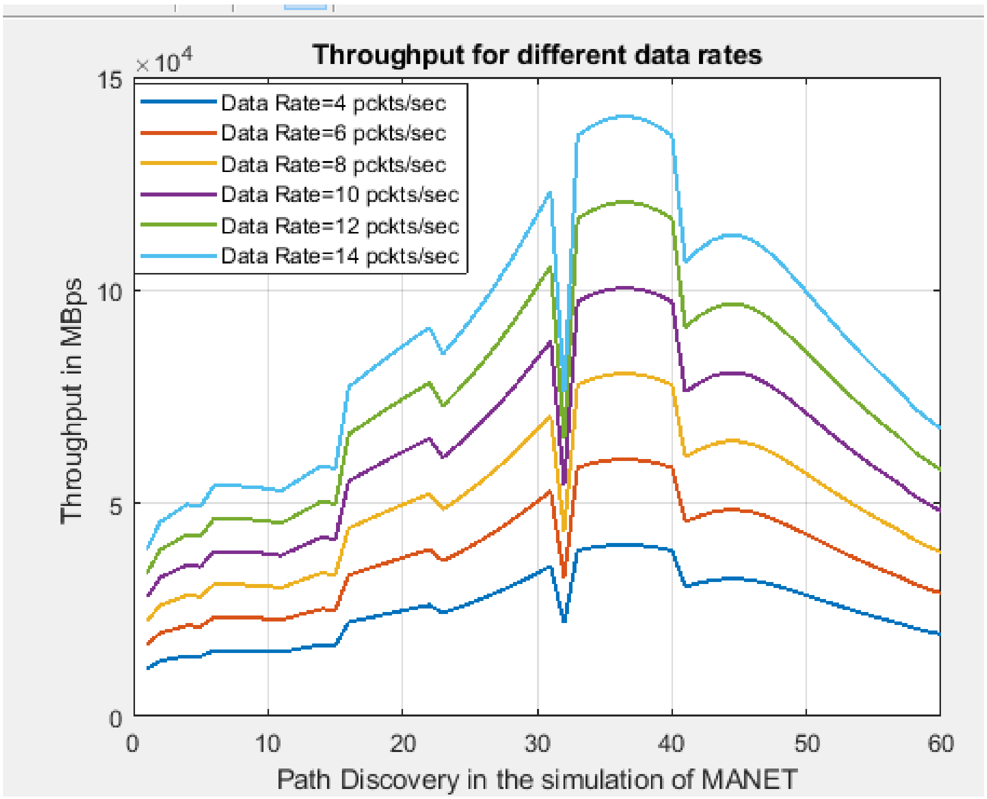


Figure 6. The results for the anomaly detection in the throughputs of the data rates in the network.

Key performance indicator

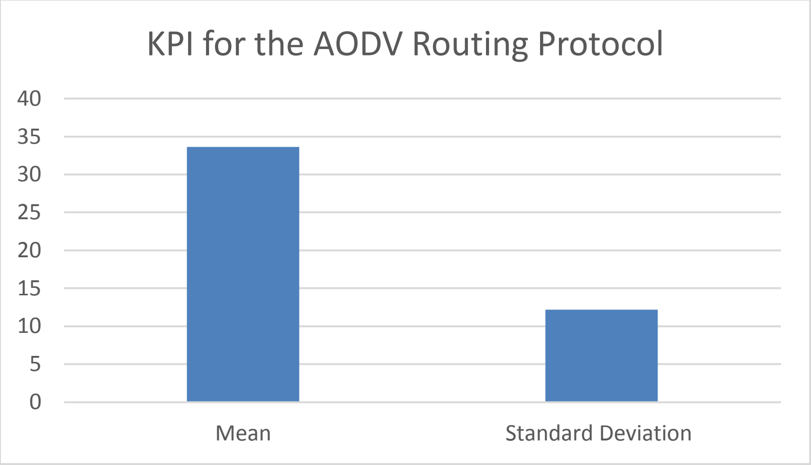


Figure 7: The KPI for the AODV routing protocol showing anomalies

The AODV protocol is capable of multicast or unicast when the source node once to transmit it will create an RREQ which will be sent via the intermediate nodes to the destination. A unicast would be used to transmit a route reply message to establish the passage of conveyance between the two nodes. In this simulation, it is evident that there was anomaly detected between the source point (20) and the target node (40). The energy consumption illustrated in figure 4 shows that there was a surge between node 30 and 40 indicating that that was increased traffic requiring more energy. This abrupt changes in the network characteristics such as the network life and throughput demonstrated in figure 5, and 6 show that the network changed drastically between node 30 and 40. After the detection process, the KPI technique was utilized to determine the presence of anomalies in the network. Figure 6 shows that the mean is greater than the standard deviation; therefore, the KPI illustrate that the communication within the cell is anomalous. The simulation scenario of the source and the destination can be associated with mobile communication in a cell with the source being the Base station and destination the user equipment. The users are used as nodes in MANETS for the hoping of traffic. The test has also shown that the reactive protocol technique shows that the proposed unified user profiling in MANETs is possible. This user profiling can easily be used to detect attacks in these ad-hoc networks. The combination of the reactive routing schemes with the KPI technique has confirmed that most network encounter anomalies but may be considered as positive false hence there is the need for a verification system to determine the authenticity of any attack alert system.

5. Conclusion

This research has presented a simple reactive protocol-based approach for user and traffic profiling in detecting anomalous communication. The AODV routing protocol can be used in emerging communication technologies to communicate between nodes. The routing protocol described the communication between a base station and user equipment. The user equipment will form the nodes for traffic routing in MANETs where traffic should be monitored constantly to detect any slight changes to avoid attacks in mobile communication. Most anomaly detection system sends positive false therefore in this study we created a key performance indicator system that would validate the anomaly as legitimate.

References

[1] M. S. Parwez, D. B. Rawat and M. Garuba, "Big data analytics for user-activity analysis and user-anomaly detection in mobile wireless network," IEEE Transactions on Industrial Informatics, vol. 13, no. 4, pp. 2058-2065, 2017.

[2] P. N. Reddy, C. Vishnuvardhan and V. Ramesh, "An Overview on Reactive Protocols for Mobile Ad-Hoc Networks," International Journal of Computer Science and Mobile Computing, vol. 2, no. 5, pp. 368-375, 2013.

[3] M. Wang and S. Handurukande, "Anomaly Detection for Mobile Network Management," International Journal of Next-Generation Computing, vol. 9, no. 2, pp. 81-97, 2018.

[4] L. Bodrog, M. Kaj´o, S. Kocsis and B. Schultz, "Robust Algorithm for Anomaly Detection in Mobile Networks," in 6th International Workshop on Self-Organizing Networks, Budapest, Hungary, 2016.

[5] R. B¨uschkes, D. Kesdogan and P. Reichl, "How to Increase Security in Mobile Networks by Anomaly Detection," in Proceedings 14th Annual Computer Security Applications Conference, Aachen, Germany, 1998.

[6] M. H. Kamarudin, C. Maple, T. Watson, and N. S. Safa, "A New Unified Intrusion Anomaly Detection in Identifying Unseen Web Attacks," Security and Communication Networks, no. 2539034, pp. 1-18, 2017.

[7] R. Kaur and S. Singh, "A survey of data mining and social network analysis based anomaly detection techniques," Egyptian Informatics Journal, vol. 17, p. 199–216, 2016.

[8] A. H. Lashkari, M. Chen and A. A. Ghorbani, "A Survey on User Profiling Model for Anomaly Detection in Cyberspace," Journal of Cyber Security and Mobility, vol. 8, no. 1, p. 75–112, 2018.

[9] S. Kalwar, "Introduction to reactive protocol," IEEE Potentials, vol. 29, no. 2, pp. 34-35, 2010.

[10] P. Grant and H. Ashman, "Anomaly detection over user profiles," in Proceedings of the 8th Australian Information Security Management Conference, Adelaide, Australia, 2010.

[11] M. Grčar, D. Mladenič, and M. Grobelnik, "User Profiling for Interest-focused Browsing History," in Proceedings of the Workshop on End User Aspects of the Semantic Web, Ljubljana, Slovenia, 2005.

[12] A. Ortigosa, R. M. Carro and J. I. Quiroga, "Predicting user personality by mining social interactions in Facebook," Journal of Computer and System Sciences, vol. 80, no. 1, pp. 57-71, 2014.

[13] M. Corney, G. Mohay and A. Clark, "Detection of Anomalies from User Profiles Generated from System," in Proceedings of the Ninth Australasian Information Security Conference, Perth, Australia, 2011.

[14] X. Luo, X. Di, X. Liu, H. Qi, J. Li, L. Cong, and H. Yang, "Anomaly Detection for Application Layer User Browsing Behavior Based on Attributes and Features," Journal of Physics: Conference Series, vol. 1069, no. 1, p. 012072, 2018.

[15] Abdulshaheed, H.R., Binti, S.A., and Sadiq, I.I., 2018. Proposed a Smart Solutions Based-on Cloud Computing and Wireless Sensing. International Journal of Pure and Applied Mathematics, 119 (18), pp.427–449.

[16] Barazanchi, I. Al, Shibghatullah, A.S., and Selamat, S.R., 2017. A New Routing Protocols for Reducing Path Loss in Wireless Body Area Network (WBAN). Journal of Telecommunication, Electronic and Computer Engineering model, 9 (1), pp.1–5.

[17] Abdulshaheed, H.R., Binti, S.A., and Sadiq, I.I., 2018. A Review on Smart Solutions Based-On Cloud Computing and Wireless Sensing. International Journal of Pure and Applied Mathematics, 119 (18), pp.461–486.

[18] B. Durakovic, “Thermal Performances of Glazed Energy Storage Systems with Various Storage Materials: An Experimental study”, Sustainable Cities and Society, vol. 45, pp. 422-430, 2019.

[19] B. Durakovic, “Design for Additive Manufacturing: Benefits, Trends and Challenges”, Periodicals of Engineering and Natural Sciences (PEN), vol. 6, pp. 179–191, 2018.

[20] B. Durakovic, Demir, R., Abat, K., and Emek, C., “Lean Manufacturing: Trends and Implementation Issues”, Periodical of Engineering and Natural Sciences, vol. 6, no. 1, pp. 130-143 , 2018.

[21] B. Durakovic, "Design of Experiments Application, Concepts, Examples: State of the Art," Periodicals of Engineering and Natural Scinces, vol. 5, no. 3, p. 421–439, 2017.