an empirical model for the investigation of effective intrusion detection systems by using k-nearest neighbor (knn) and fuzzy (fuzzy knn) algorithms in mobile ad-hoc network (manet)

Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, October 2021: 1569-1578

An Empirical Model for the Investigation of Effective Intrusion Detection Systems by Using K-Nearest Neighbor (KNN) and Fuzzy (Fuzzy KNN) Algorithms in Mobile Ad-Hoc Network (MANET)

[1]N.C.SendhilKumar* ,[2]Amedapu Srinivas,[3]N.Selvaganesh, [4]C.Senthilkumar, [3]S.Ravi Chand

[1]Professor, Department of Electronics and Communication Engineering, Sri Indu College of Engineering & Technology, Sheriguda Hyderabad, Telangana 501510.
[1]Email:sendhilkumarnc@gmail.com
[2]Associate Professor,Department of Computer Science and Engineering,Sreenidhi Institute of Science and Technology,Ghatkesar, Hyderabad – 501301,Telangana.
[2]Email : SrinivasReddyAmedapu@yahoo.com
[3]Assistant Professor, Department of Computer Science and Engineering, PSNA College of Engineering and Technology,Kothandaraman Nagar, Dindigul-624622, Tamil Nadu
[3]Email: selva492@gmail.com@gmail.com
[4]Aistssant Professor (S.G), Department of Electronics and Communication Engineering, Saveetha School of Engineering (Saveetha University), Chennai- 602105, Tamilnadu
[4]Email: senswain@gmail.com
[5]Professor, Department of Electronics and Communication Engineering
Nalla Narasimha Reddy Education Society's Group of Institutions - Integrated campus, Hyderabad, Telangana- 500088
Email: ravichandsankuru1@gmail.com

Abstract

A mobile ad hoc network (MANET) is a high-speed network that does not have any infrastructure or centralized management. In recent years, MANET has been popular and widely used by various applications. The important concern of MANET is security. In MANET, Intrusion detection systems (IDSs) are a prominent solution for achieving security. Among these, Clustering-based IDSs are highly noticeable mainly for their proper scalability behaviors. In this paper, the K-nearest neighbor (KNN) algorithm with fuzzy (Fuzzy KNN) inference is proposed to detect the MANET's black hole attack. The implementation of fuzzy inference is effective in the selection of cluster heads. Additionally, Josang mental logic along with beta distribution increases each node's trustiness. The destination node detects by the trust servers using the reputation and remaining energy. In each cluster, the cluster head is responsible for detecting the node which involved in suspicious activity like black hole attack. The proposed work performance is examined using parameters like total network delay, throughput, packet loss rate, and normalized routing load. The obtained result proves that the proposed system is very effective in detecting the black hole than the other methods.

Keywords: MANET, Intrusion Detection, KNN, Cluster Mechanism,IDS

1. Introduction

Technology evolution and its advancement rise to new heights within a short period. The networking technology is the most noticeable one that provides data exchange from one medium to another. Commonly, the centralized system manages the network, and the emergence of MANET gives rise to an infrastructure-less environment. MANET is referred to as a Mobile Ad hoc Network, which has

been very popular in recent years. MANET is a wireless communication that delivers communication or information exchange among the mobile nodes connected as a network. The node connection with another and its arrangement is described as infrastructure less. MANET comprises various features which make its presence on multiple applications widely. Those applications are crucial in real-time scenarios such as rescue operations, virtual conferencing, military, education, etc. In MANET, each device contains a receiver and transmitter for communication between one device to another. MANET is generally mobility in nature which does not consider the communication range of the devices that participated in the communications. MANET is divided into two networks, such as single-hop and multi-hopnetworks.

Single hop networks mean all nodes are user connected directly within the same range for establishing the communications. The multi-hop network allows communication with different fields utilizes intermediate devices for successful communications.

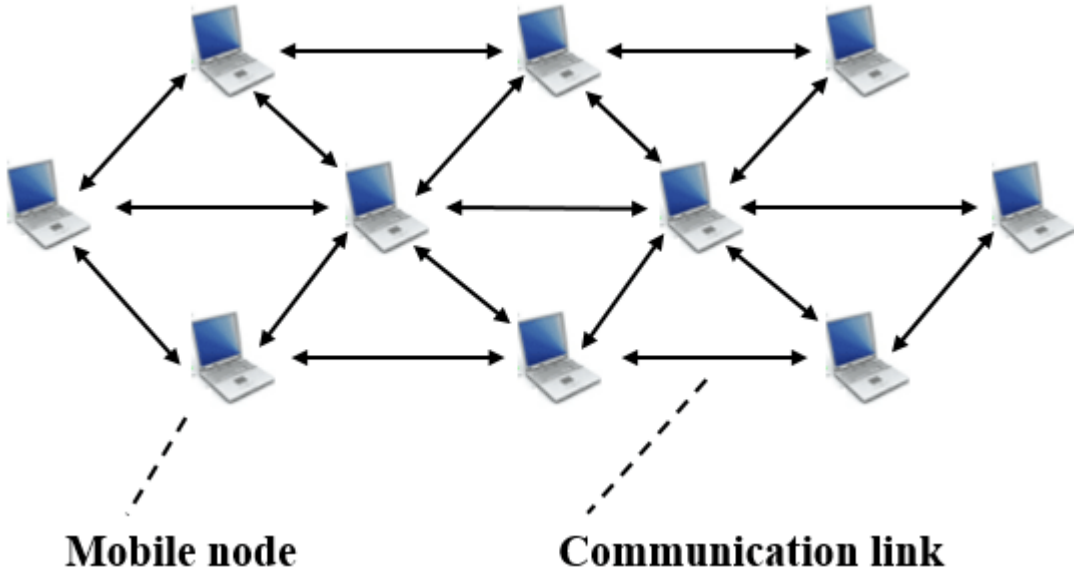

Figure 1. MANET Architecture

MANET attacks are possible due to two reasons; the first one is its wireless nature. It makes it complex in identifying the attacks or tracking anonymous users. Secondly, MANET is an open medium; there is no restriction on joining and relieving anybody at any time. To assure network security is essential an efficient mechanism for identifying the attacks. That too identification of attacks needs to be done before its occurrence, which will be more beneficial. Intrusion Detection System (IDS), a prominent detection mechanism that effectively detects unauthorized entities' activities or any un-approved access. MANET with IDS involves two concepts such as intrusion detection architecture and Intrusion detection technique.

1.1 Intrusion Detection System (IDS)

IDS is mainly responsible for intrusion detection on the audited data. In the network, gathered data are referred as audited data. The primary IDS is responsible for response, detect, monitor and evaluate. IDS classification is done as network-based or host-based. For MANETs, Network-based IDSs are not applicable as it needs monitoring or data collection, which is communicated via network hardware

interface. Host-based IDSs based on the user-generated data or programs present in the host. IDSs software is installed on all systems individually and operated separately, perfect for MANETs [1]. MANET contains various complexities that make typical IDS useless for the new environments. This makes the research community for developing the new IDSs or enhance the performance of the existing systems.

2. RELATED WORK

Poongudi et al [1], proposed Localized Secure Architecture for handling the black hole attacks in MANET. Security Monitoring Nodes (SMNs) are used here for detecting the malicious nodes in the network. Kumar et al [2], proposed a combined hybridization system with fuzzy and GA algorithm for handling the Black hole attack in AODV. The main objective of this system is to avoid the presence of malicious nodes in the network, as it is the major reason for various types of attacks. Shahabi et al [3], proposed a modified algorithm for enhancing the security against the black hole attacks. This system effectively detects the nodes behaviors and identifies the black hole attacks. It removes the malicious nodes from routing. Somasundaram et al [4], proposed a Crypto-key based Black Hole Detection and Avoidance Protocol (CBHDAP). This algorithm facilaites group key mechanism using Diffie-Hellman (DH) based key agreement system. It is effective in the detection and avoiding the black hole attacks.

Arathy et al [5], proposed D-MBH algorithm for identifying the single and multiple black hole in the network. The black hole list is created using threshold ADSN and minimize the computational along with routing overheads. Dumne et al [6], proposed advanced detection method using DSR mechanism-cooperative bait detection scheme (CBDS). It is a hybrid approach applies reverse tracing technique for identifying the malicious nodes effectively. Nitnaware et al [7], proposed Dynamic MANET On-Demand (DYMO) routing protocol for addressing the black hole attack in the network. In this system, a mitigation algorithm is discovered for deciding the genuine of the nodes in the network. Tamilselvi et al [8], proposed an advanced routing discovery process in data transmissions. This route discovery mechanism does not check the black hole list regularly because it does not maintain any black hole lists. The proposed routing system removes the black hole node and for transmission only reliable nodes are used.

FarooqAnjum et al. proposed an initial approach to detect intrusions in ad hoc networks. AnandPatwardhan et al. proposed a secure routing protocol based on AODV over IPv6, further reinforced by a routing protocol independent Intrusion Detection and Response system for ad hoc networks. Tseng (2006) proposed a complete distributed intrusion detection system has consisting of four models for MANETs with formal reasoning. Fahad & Robert ask with concentrated on the detection phase and they have proposed a mechanism Packet Conservation Monitoring Algorithm (PCMA) which is used to detect selfish nodes in MANETs.

Meka et al. Proposed a trust based framework to improve the security and robustness of ad hoc network routing protocols. For constructing their trust framework, they have selected the Ad hoc on demand Distance Vector (AODV) which is popular and widely used. Making minimum changes for implementing AODV and attaining increased level of security and reliability is their goal. Their schemes are based on incentives &penalties depending on the behavior of network nodes. Their schemes incur minimal additional overhead and preserve the lightweight nature of AODV. Shiqun Li

et al. explored that the security issues of wireless sensor networks, proposed an efficient link layer security scheme. To minimize computation and communication overheads of the scheme, they have designed a lightweight CBC-X mode Encryption/Decryption algorithm that attained encryption/decryption and authentication all in one. They have also devised a novel padding technique, enabling the scheme to achieve zero redundancy on sending encrypted/authenticated packets. As a result, security operations incur no extra byte in their scheme.

Zhang et al. Proposed a Credit-Based Secure Incentive Protocol (SIP) to stimulate cooperation in packet forwarding for infrastructure less MANETs. Liu et al. proposed the 2ACK scheme that has served as an add-on technique for routing schemes to detect routing misbehavior and mitigate their adverse effect Li Zhao & Delgado-Frias proposed a scheme MARS scheme and its enhancement E-MARS Scheme to detect misbehavior and mitigate adverse effects in ad hoc Networks. Afzal et al. explored that the security problems and attacks in existing routing protocols and they have presented the design and analysis of a secure on-demand routing protocol, called RSRP which confiscated the problems mentioned in the existing protocols. In addition, RSRP has used a very efficient broadcast authentication mechanism which does not require any clock synchronization and facilitates instant authentication. Patwardhan et al. proposed an approach to secure a MANET by using a threshold-based intrusion detection system and a secure routing protocol. Madhavi & Kim proposed a MIDS (Mobile Intrusion Detection System) suitable for multi-hop ad-hoc wireless networks, which have detected nodes misbehavior, anomalies in packet forwarding, such as intermediate nodes dropping or delaying packets. Bhalaji et al. Proposed an approach based on the relationship between the nodes to make them cooperate in an ad hoc environment. The trust values of each node in the network are calculated by the trust units. The relationship estimator has determined the relationship status of the nodes by using the calculated trust values. Their proposed enhanced protocol is compared with the standard DSR protocol and the results are analyzed by using the Network Simulator 2.In Mergen et al. suggested reliable data fusion in wireless sensor networks considered with mobile access points (SENMA) under both static and dynamic Byzantine attacks, where which the malicious nodes report false evidence with a fixed or time-varying possibility, respectively. In SENMA, the mobile access point (MA) traverses the network and collects the sensing information from the individual sensor nodes.

The adversary has full control over some of the authenticated nodes and can perform arbitrary behavior to disrupt the system (Awerbuch et al. 2004).Furthermore, if the sensing reports represent a hard-decision (’yes’ or ’no’), it has been shown that by using the OR rule to find the final sensing decision it leads to a very high false alarm probability. The approach is to moderate the Byzantine attacks by using the q-out-of-m scheme, for which the final decision is based on q sensing reports out of m, polled nodes. This makes the q-out-of-m scheme a potential applicant for large scale sensor networks. Further the examined performance of this approach is under both static and dynamic attacking strategies (Abdelhakim et al. 2011).

3. Proposed work

(a) K-nearest neighbor (KNN) algorithm

In data mining, the KNN algorithm is considered as the most popular algorithm which contains minimum complicated on executing classification. The main purpose of KNN is achieving closet

values in the cluster. KNN is very efficient in handling text classification, cancer diagnosis and Pattern recognition and so on. Generally, KNN is an instance-based method or lazy learning methods. KNN labels its nearest K neighborhood based on the sample data. Each node contains its similarity score, which is considered the neighboring node cluster [9]. These weights are used for measuring the distance among neighbors effectively [10]. The KNN algorithm's main property is a single or multidimensional feature vector and measured the Euclidean distance. In the proposed system, the nodes are represented using the two-dimensional vector, and the node's distances are calculated per the Euclidean relation (1) and cluster formation.

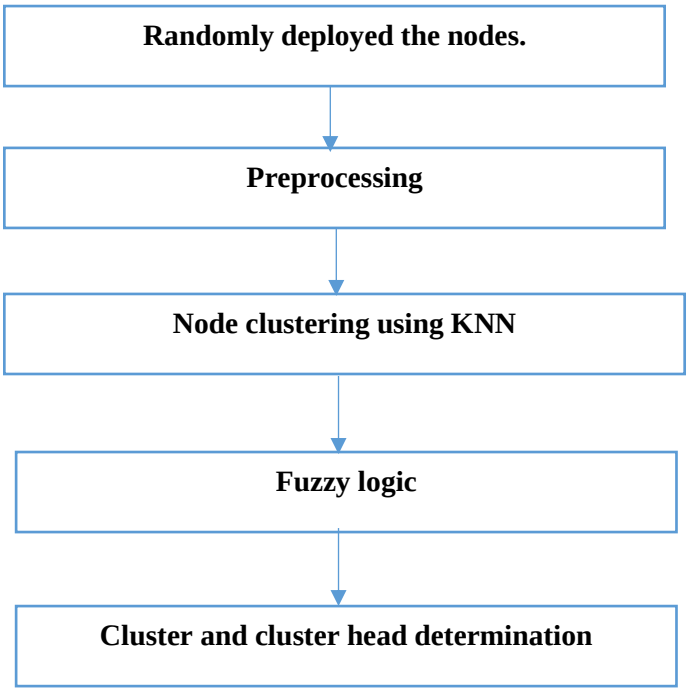

Figure 2 Proposed KNN Architecture

$$d(a, a_i) = \sqrt{(a_i - a_j)^2} \qquad (1)$$

Here the network nodes are a_i and a_j. The proposed system is used to detect attacks using KNN classification based on the learnings. One node is compared with another node to determine it also contains the same properties. Each node picks an N-dimensional space point, and in the N-dimensional pattern space, where nodes are kept. In the entire system, N is the unknown node, and the KNN begins its pattern space for searching the K known nodes near the unknown node. The unknown node of the KNN cluster is mapped with CNN's common clusters. In the algorithm, the selection of the K parameter is essential, and the value differs from within the square root of training set sizes [11]

(b) Fuzzy Logic

Implementation of fuzzy logic is easy and delivers enhanced output in the term accuracy by removing uncertainties. The elements are labeled according to classical logic as 0 or 1. In the Fuzzy set theory, the set of values falls between 0 and 1. Fuzzy logic confirms its rational decisions based on incomplete information, uncertainty, and imprecision in an environment. Fuzzy logic properties make the collected data and are applied according to the real-time scenarios with continuous-valued elements [12]. Wu and Banzhaf [34] suggest fuzzy logic for validating the network anomaly detection system (NADS). Mainly for these two reasons such as;The intrusion detection problem contains various numeric attributes which are collected from data auditing and statistical measures. On the numeric data, directly building models leads to heavy detection errors. Fuzziness includes security as the normal and abnormal boundaries are not defined properly. The primary purpose of a fuzzy inference system is the mapping of input to output. The fuzzy inference system includes the following processes [12].

(c) Fuzzification of Inputs

In fuzzy inference systems, the initial step is getting the inputs and describing their membership degree employing membership functions. The output is the fuzzy degree which represents the total input membership from the fuzzy input set. The output is described in the form of numerical values between 0 and 1.

(d) Defuzzification

A fuzzy set is the fuzzy process input and the obtained number is the output. The main intention of implementing fuzzy inference system and intrusion detection are described below;

- Capability of working in both classification and clustering.
- Expert monitoring of the learning process, ability to interpret and update the fuzzy system. The updating includes the fuzzy sets and their database rules
- Its intelligent systems contain the ability to balance the face uncertainty issues.

(e) Proposed algorithm steps (Fuzzy based KNN)

- In the network, nodes are distributed randomly with unique ID
- Cluster formation is done between the nodes. The cluster Ci and cluster head CH is chosen by employing the KNN algorithm and fuzzy inference
- Si is the source node request the head CH for path to identify the destination
- CH cluster head monitors the nodes of its cluster either they are finding the destination Di correctly or not. If the destination is not identified properly means a request sent to other cluster head to identify the shortest path.
- On reaching the destination each node responses to the CH
- CH replies the node’s ID to the trust server
- The obtained destination ID is verified by the trust server and replies to the cluster head. If the ID is not valid means it’s added to the blacklist and notifies the other CH for updating their blacklists. Step is repeated.
- End.

4. Result and Discussion

NS-2, Network simulator is used for executing the proposed Fuzzy-KNN. The simulation set up is built with 120 nodes among 1700 × 1700 m^2. A dynamic network is used, crated through the Random way mobility model. This model enables to move the nodes in the network anywhere. In this set-up, the link-layer protocol is the IEEE standard of 802.11 Mac protocol. The multicast constant bit ratio is used for generating the network traffics. The heterogeneous traffic such as both 802.11b and IEEE 802.11e WLAN are considered in this work. The TCP or UDP network topology is used for the data connections. The packet used for transmission is 2000 bytes in size with a data rate of 24 Mbps. The below table list the other parameters used in the experimental work.

Table 1 Simulation Parameters

Parameter	Assigned value
Number of Nodes	100
Sensing Region	1000 m × 1000 m
Initial Node Energy	1000J
Packet Size	512B
Transmission Power	0.02Watts
Received Power	0.01Watts
Routing Protocol	DSR
Data Rate	1Mbps
Radio-Propagation Model	Two Ray Ground

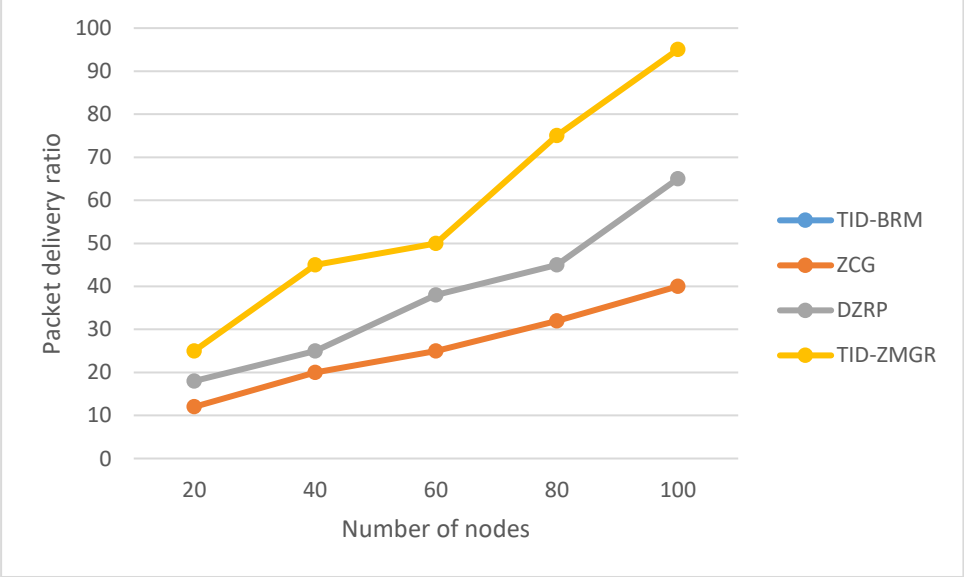

Figure 3: PDR vs. number of nodes

The above figure 3 shows the comparison work carried out on packet delivery ratio (PDR) with a number of nodes used. Comparison work is done between the proposed FUZZY-KNN with AODV and Crypto key-based black hole detection and avoidance protocol (CBHDAP). The x-axis states the number of nodes used, and the y-axis states the obtained PDR. The number of nodes used is gradually increased in the count of 20 at regular intervals. The proposed TID-BR FUZZY-KNN achieves a PDR of 25% with 20 nodes, PDR of 45% with 40 nodes, PDR of 50% with 60 nodes, PDR of 75% with 80 nodes, and PDR of 95% with 100 nodes. Whereas ADOV achieves PDR of 18% with 20 nodes, PDR of 25% with 40 nodes, PDR of 38% with 60 nodes, PDR of 45% with 80 nodes, and PDR of 65% with 100 nodes. In contrast, CBHDAP achieves a PDR of 12% with 20 nodes, PDR of 20% with 40 nodes, PDR of 25% with 60 nodes, PDR of 32% with 80 nodes, and PDR of 40% with 100 nodes. It clearly shows the proposed FUZZY-KNN performance on PDR is far better than the others.

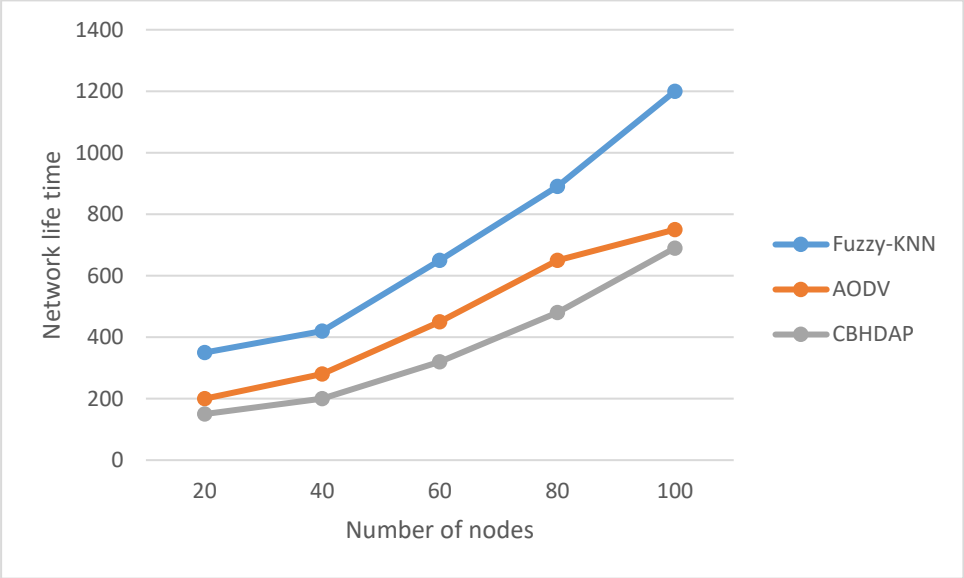

Figure 4: Network lifetime vs. number of nodes

The above figure 4 shows the comparison work carried out on network lifetime with a number of nodes used. Comparison work is done between the proposed FUZZY-KNN with AODV and Crypto key based black hole detection and avoidance protocol (CBHDAP). The x-axis states the number of nodes used and y-axis states the obtained network life time. The network life time is calculated in terms of sec. The number of nodes used is gradually increased in the count of 20 at regular intervals. The proposed TID-BR FUZZY-KNN achieves 350 secs of network lifetime with 20 nodes, 420 secs of network lifetime with 40 nodes, and 650 secs of network lifetime with 60 890 secs of network lifetime with 80 nodes and 1200 secs of network lifetime with 100 nodes.
In contrast, AODV achieves 200 secs of network lifetime with 20 nodes, 280 secs of network lifetime with 40 nodes, 450 secs of network lifetime with 60 nodes, 650 secs of network lifetime with 80 nodes, and 750 secs of network lifetime with 100 nodes. The CBHDAP achieves 150 secs of network lifetime with 20 nodes, 200 secs of network lifetime with 40 nodes, 320 secs of network lifetime with 60 nodes, 480 secs of network lifetime with 80 nodes, and 690 secs of network lifetime with 100 nodes. It clearly shows that the proposed FUZZY-KNN achieves a maximum network lifetime than the others.

5. Conclusion

In this paper, security issue especially black hole attack is addressed by implementing the proposed FUZZY- KNN algorithm. MANET is one of the popular technologies which has a rapid growth in the recent years. The identification of black hole attacks is very difficult because of MANET characteristics like open medium and infrastructure-less medium. The proposed system combines the K-nearest neighbor (KNN) algorithm for clustering and fuzzy inference for cluster head selections. To examine the performance of the proposed work, a comparison work is carried out between the proposed FUZZY-KNN with AODV and CBHDAP. The evaluation metrics considered are PDR and network lifetime. The obtained results are graphically plotted for observation. The comparison results show that the proposed FUZZY-KNN has enhanced performance on PDR and network lifetime than the other algorithm. It clearly shows that the proposed system's fuzzy inference early detection of any black hole attacks and its quick intimation to cluster head in the network.

Reference

1. Poongodi, T., &Karthikeyan, M. (2016).Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks.Wireless Personal Communications, 90(2), 1039–1050. https://doi.org/10.1007/s11277-016-3318-5
2. Kumar, R., &Chadha, R. (2016).Mitigation of black hole attack using genetic algorithms and fuzzy logic.International Journal of Engineering Sciences & Research Technology, 5(6), 818–826.
3. Shahabi, S., Ghazvini, M., &Bakhtiarian, M. (2016).A modified algorithm to improve security and performance of AODV protocol against black hole attack.Wireless Networks, 22(5), 1505–1511. https://doi.org/10.1007/s11276-015-1032-y
4. Kumar, K. V., &Somasundaram, K. (2016).An effective CBHDAP protocol for black hole attack detection in MANET.Indian Journal of Science and Technology, 9(36)
5. Arathy, K. S., &Sminesh, C. N. (2016).A novel approach for detection of single and collaborative black hole attacks in MANET.Procedia Technology, 25, 264–271. https://doi.org/10.1016/j.protcy.2016.08.106
6. Dunne, P. R., &Manjaramkar, A. (September2016).Cooperative bait detection scheme to prevent collaborative blackhole or gray hole attacks by malicious nodes in MANETs. InProceedings of the International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), Noida, India.
7. Nitnaware, D., &A. (February2016). akur, "Blackhole attack detection and prevention strategy in DYMO for MANET," in Proceedings of the International Conference on Signal Processing and Integrated Networks.Noida, India.
8. Tamilselvi, P., &Ganesh Babu, C. (2019).An efficient approach to circumvent black hole nodes in manets.Cluster Computing, 22(S5), 11401–11409. https://doi.org/10.1007/s10586-017-1395-1
9. Taneja, S., Gupta, C., Goyal, K., &Gureja, D. (February2014).An enhanced k-nearest neighbor algorithm using information gain and clustering. InProceedings of the International Conference on Advanced Computing and Communication Technologies, Rohtak, India.
10. Yusof, A. R., Udzir, N. I., &Selamat, A. (August2016).An evaluation on KNN-SVM algorithm for detection and prediction of DDoS attack. In. Lecture Notes in Computer Science.Proceedings of the International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, Morioka, Japan, 95–102. https://doi.org/10.1007/978-3-319-42007-3_9

11. Hassanat, A. B., Abbadi, M. A., Altarawneh, G. A., &Alhasanat, A. A. (2014).Solving the problem of the k parameter in the KNN classifier using an ensemble learning approach.International Journal of Computer Science and Information Security, 12(8), 33–39.
12. Hamamoto, A. H., Carvalho, L. F., Sampaio, L. D. H., Abrão, T., &Proença, M. L. (2018).Network anomaly detection system using genetic algorithm and fuzzy logic.Expert Systems with Applications, 92, 390–402. https://doi.org/10.1016/j.eswa.2017.09.013
13. Farooq Anjum, DhanantSubhadrabandhu&Saswati Sarkar 2003, 'Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols',In proceedings of IEEE 58th Conference on Vehicular Technology.
14. Zhang, Y, Wenjing Lou, Wei Liu & Yuguang Fang 2007, 'A secure incentive protocol for mobile ad hoc networks', Wireless Networks (WINET), vol. 13, no. 5.
15. Farooq Anjum, DhanantSubhadrabandhu&Saswati Sarkar 2003, 'Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols', In proceedings of IEEE 58th Conference on Vehicular Technology.
16. Zhang, Y, Wenjing Lou, Wei Liu &Yuguang Fang 2007, 'A secure incentive protocol for mobile ad hoc networks', Wireless Networks (WINET), vol. 13, no. 5.
17. Awerbuch, B, Curtmola, R, H. D., N.R. C., and R.H. 2004, 'Mitigatingbyzantineattacksinadhoc wireless networks', Technical report version 1.
18. Mergen, G, Qing, Z & Tong, L 2006, 'Sensor networks with mobile access: energy and capacity considerations', IEEE Trans. Comm., vol. 54, no. 11, pp. 2033-2044.
19. Bhalaji, Sivaramkrishnan, Sinchan Banerjee, Sundar&Shanmugam 2008, 'Trust enhanced dynamic source routing protocol for adhoc networks', in proceedings of World Academy Of Science, Engineering and Technology, vol. 36, pp. 1373-1378.
20. Li Zhao & Delgado-Frias, JG 2007, 'MARS: Misbehavior detection in ad hoc networks', In proceedings of IEEE Conference on Global Telecommunications Conference.
21. Meka, KM, Virendra&Upadhyaya 2006, 'Trust based routing decisions in mobile ad-hoc networks', In Proceedings of the Workshop on Secure Knowledge Management
22. Shiqun Li, TieyanLi,Xinkai Wang, Jianying Zhou &Kefei Chen 2007, 'Efficient link layer security scheme for wireless sensor networks', Journal of Information And Computational Science, vol. 4, no. 2, pp. 553-567.
23. Shiqun Li, TieyanLi,Xinkai Wang, Jianying Zhou &Kefei Chen 2007, 'Efficient link layer security scheme for wireless sensor networks', Journal of Information And Computational Science, vol. 4, no. 2, pp. 553-567
24. Farooq Anjum, Dhanant Subhadrabandhu &Saswati Sarkar 2003, 'Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols', In proceedings of IEEE 58th Conference on Vehicular Technology
25. Chin-Yang Henry Tseng 2006, 'Distributed intrusion detection models for mobile ad hoc networks', University of California at Davis Davis, CA, USA.