ISSN 2347 - 3983
Volume 9. No. 6, June 2021
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter13962021.pdf
https://doi.org/10.30534/ijeter/2021/13962021

A Proposed AODV Black hole Detection Model using the Fuzzy Inference Method in MANET Topology

Chigozirim Ajaegbu[1], Kelechi C. Umeaka[2], Kenneth T. Nwala[3], Frank B. Osang[4]
[1]Department of Computer Science, Babcock University, Nigeria. ajaegbuc@babcock.edu.ng
[2]Department of Computer Science, Babcock University, Nigeria. ajaegbuc@babcock.edu.ng
[3]Department of Mathematics and Computer Science, Clifford University, Nigeria, nwalat@cliffordduni.edu
[4]Department of Computer Science, National Open University, Nigeria, fosang@noun.edu.ng

ABSTRACT

Mobile Adhoc Network (MANET) as a network of mobile routers that self-configures has raised some security concerns which one of them has been the Black Hole Attack (BHA). Studies have shown various detection and mitigation techniques in line with the black hole attack of MANET technology. However, some of the proposed models in this direction have paid less attention to how fuzzy systems could be integrated in Adhoc On-Demand Distance Vector (AODV) protocol, to further guide its detection abilities against a possible black hole attack. Hence the study proposed a model that integrates the Fuzzy Inference Method (FIM) on the existing AODV security measures in order to strengthen further its detection metrics. Also, an Intrusion Detection System (IDS) was introduced for an early check against possible BHA along with the Fuzzy Parameter Extraction module which performs all necessary parameter checks before passing it on to the FIM. The parameters into consideration were adapted from the study of Narang (2013), with this study modifying further its proposed algorithm using the added concepts earlier mentioned. The proposed model presented tends to perform better than the existing models in this direction with evidence from the theoretical underpinnings of the functionality of the added modules in the proposed system.

Key words: Adhoc On-Demand Distance Vector (AODV), Black Hole Attack (BHA), Fuzzy Inference Method (FIM), Mobile Adhoc Network (MANET),Intrusion Detection System (IDS).

1. INTRODUCTION

A network has been seen as an instantiation of a graph [1] that has shown applications in wireless network such as MANET. MANET has given an upward push to the dynamics of wireless sensor network in the sense that, the nodes in MANET is self-configuring and does not need any fixed infrastructure hence; every node in the network has the ability to embark on direct communication to any other node with the help of the nearest node serving as intermediate node. With this, communication among nodes in MANET is limited within short range transmission. This however, has resulted in studies around developing and proposing routing protocols such as AODV, Secure AODV (SAODV), Blackhole Protected AODV (BP-AODV) and so on; that should inform shortest paths between communicating nodes within the network.

Studies have shown that MANET topology still lacks in some areas of general performance hence, the drive for various studies such as: [1], looked at an improved version of overcrowding control using Adhoc On-Demand Multipath Distance Vector with the origin node electing a neighbour node to partake in the routing process as against other existing nodes in the network. Reference [2], carried out a review study in the direction of challenges surrounding the integration of the internet within the MANET technology. Their studies went further to recommend ways the technology could be implemented along with wired networks. Reference [3] looked at distributed scheduling schemes for a topology-transparent MANET in order to accommodate delay-constrained traffic for the first time. They also looked at and contrasted probabilistic ALOHA schemes and deterministic sequence schemes, such as Time Division Multiple Access (TDMA) and the Galois Field (GF) sequence scheme, which contributed to their proposed scheme for a particular kind of sparse network topology. Reference [4] suggested MiabNET, a novel MANET protocol built on the concept of "message-in-a-bottle" in his article. This protocol is reactive, requiring just a small amount of overhead for path requests. Through assisting source nodes in locating their target, middle nodes are able to upgrade their routing tables, reducing the number of hops available for packet forwarding and increasing the efficiency of the entire network. Reference [5] investigated the impact of a Distributed Danial of Service (DDoS) attack on a number of MANET protocols, including the Zone Routing Protocol (ZRP), Adhoc On-Demand Distance Vector (AODV) protocol, and Location-Aided Routing (LAR). According to their findings, ZRP outperformed other presented protocols in terms of showing the most DDoS resistance behavior. Reference [6] developed a model known as Student Social Based Mobility Model (SSBMM) for the purpose of inspiring the daily life of students. The proposed model was evaluated using social relation mobility model tools to ensure its proper workability. Reference [7] proposed a system known as Modified AODV (M-AODV) with the intention of implementing an overhearing backup protocol that leverages on the existing MANET

protocol (AODV). Their result showed improvement in the direction of packet delivery ratio, reduction in transmission delay while increasing the amount of overhead. Reference [8] focused on the development of a model that will ensure reliability and energy efficiency for MANET multicasting. Furthermore, the authors stated that their model performed better in terms of efficiency, packet distribution ratio, energy usage, and throughput. Reference [9] proposed Particle Swarm Optimization (PSO) model for the purpose of augmenting existing anomaly detection models proposed by researchers in the past. Reference [10] looked at ways that MANET communication strategies could be employed during emergency and disaster situations. Hence, authors provided an overview of existing MANET protocols that is best employed during secure and rescue operations. The interface between wireless sensors, MANET, and the Internet of Things, according to [11], opens up a new model in the development of MANET-IoT systems. Hence, the authors proposed a routing technique that should accommodate Internet of Things technology along with MANET and WSN technologies. In their paper, [12] stated that a systemic method might be used to analyze the routing attacks that occur in complex source routing protocols, so the authors decided to investigate the trust dependent routing protocol. The authors have presented a basis for a comparative analysis of the numerous current trust-based routing protocols. Reference [13] carried out a two-case study on the techniques of video streaming over MANETs and their study identified that video quality and Quality of experience are dependent on node density and their speed within the MANET network. Reference [14] embarked on the study of a range of MANET routing protocols in the direction of their various characteristics and functionalities.

Data transmission in MANET, employs some routing mechanism such as proactive, reactive and hybrid routing protocol. In MANET topology, nodes experience some sort of free movement and this ascertains its design principle of exercising mobility among nodes. Regardless of the mobility advantages of MANET nodes, the network is vulnerable to a variety of security attacks, several of which have been listed in the literature, such as the Gray hole attack, Black hole attack, Selective Packet Drop attack (which is often attributed to the Gray hole attack), and so on.

This study focuses on the Black hole attack on MANET topology and proposes a further way to facilitate its early detection and mitigation.

2. RELATED WORKS

According to [15], the absence of infrastructure and unified control in MANET technology exposes MANET to Black hole attacks. As a result, the authors suggested a method focused on weighted binary relational fuzzy trust to protect the AODV protocol from black hole attacks.

Reference [16] implemented a honeypot technique that included several algorithms, resulting in a black hole attack security approach known as honeypot-based anomaly detection with cross layer defense. As contrasted to other current strategies, the authors identified a better methodology in terms of packet distribution and end-to-end latency.

Reference [17] investigated and updated the current on-demand routing protocol Temporally-Ordered Routing Algorithm (TORA), and suggested Secured TORA to identify and avoid black hole attack behavior in MANET topologies.

Due to its design principles, [18] believe that data transmission among nodes in a MANET network should include protection implementation. As a result, the researchers suggested a cluster-based attack identification and avoidance strategy.

The Dynamic MANET On-Demand routing protocol, according to [19], was developed to be an upgrade on the current AODV protocol with the aim of enhancing the network's overall efficiency. As a result, the developers suggested an algorithm aimed at preventing and minimizing black hole attacks on legitimate nodes.

AODV, according to [20], is a MANET protocol that is widely recognized as one of the current routing protocols. As a result, the writers devised a novel approach for reducing black hole attacks in both independent and joint activities, requiring less routing, storage, and computing overhead.

Reference [21] investigated the impact of a black hole attacks on the accuracy of the ADOV protocol. The authors achieved their goal by varying the number of nodes involved in the network as well as the black hole node.

According to [22], AODV is one of the key MANET protocols that may be vulnerable due to malicious nodes in the network. The authors suggested a method for detecting and defending nodes against potential attack by implementing a protected route based on Normal versus Abnormal behaviour.

According to [23], Dynamic Source Routing is a reactive MANET routing protocol that uses on-demand routes and hence seems susceptible to a black hole attack. The researchers, on the other hand, looked at black hole attacks on DSR-based MANETs.

Reference [24] proposed a sequence number mechanism that functions at the source node by subjecting the route request packet (RREQ) message coming from the respective node to check in comparison with the defined threshold.

Reference [25], proposed a black hole detection and mitigation mechanism that identifies affected nodes and goes further to recommend possible way out using fuzzy rule-based technique.

3. SYSTEM MODEL

The study adopted the algorithm present by [25] with slight modification in order to demonstrate researcher’s opinion effectively. In order to detect a potential black hole attack in the network, the proposed framework uses parameters specified

by [25], such as packet loss and data rate. More specifically, the three-step priority assignment used by [25] holds true in this analysis as follows:

Step 1: If packet loss is poor but data rate is strong, priority should be set to strong.
Step 2: If the packet loss is moderate and the data rate is strong, the priority should be set to moderate.
Step 3: If packet loss and data rate are also poor, priority is also poor.

However, the major modification that this study presented is the inclusion of the following to the already existing system of [25]:

- an Intrusion Detection System (IDS) module
- a fuzzy parameter extraction
- integration of the FIM into the existing AODV protocol and
- an alarm module

As a result, the following steps instruct the functionality of the various modules:

Step 1: Assign network traffic to the IDS module
Step 2: IDS module compares received traffic parameters with threshold
Step 3: if traffic parameters equal threshold
Step 4: Repeat 1 to 3 Else
Step 5: traffic parameters not equal to threshold then
Step 6: Assign parameters to FPE module
Step 7: FPE performs necessary parameter extraction and assigns to FIM
Step 8: FIM integrated to the AODV protocol takes action by blocking further BHA operations on the network
Step 9: Alert every node participating in the network of the detected attack.

3.1Proposed Black Hole Mitigation Model

As mentioned earlier in literature that the lack of a defined infrastructure and a centralized control in MANET technology, exposes the network to attacks. Researchers also identified black hole attacks as one of the security challenges in MANET and actively seeking for ways to improve in the detection and mitigation of its activities in MANET. Also, studies have shown that AODV protocol has also received much attention as compared to other MANET protocols and this is so because it has been observed that among other MANET protocols being proposed, AODV appears to be more prone to black hole attack. Hence, this study proposes the use of a fuzzy logic reasoning method integrated into the operations of AODV protocol in order to add to its detection ability hence resulting in a huge upgrade in its security model. The fuzzy logic reasoning method in the proposed system is driven by a flexible Fuzzy Inference Method (FIM). The FIM would be capable of extracting a valuable judgment from MANET security protocols using a small amount of raw data. The successful implementation of FIM in the fuzzy logic reasoning methodand infusion into the security protocols of MANET means an air tight security against black hole attacks. See figure 1.

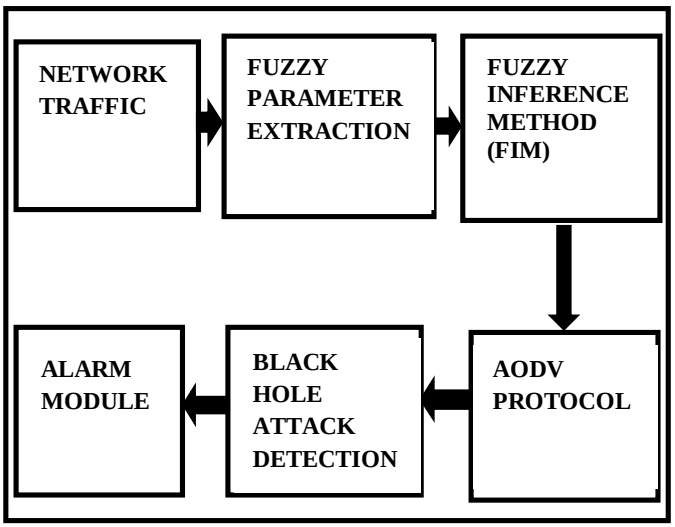

Figure 1: Researcher's proposed FIM model for Intrusion Detection

From figure 1, the Network Traffic comes into the Intrusion Detection System (IDS) which is powered by an adaptive Fuzzy Inference Method (FIM) infused with the AODV protocol. The Network Traffic enters the IDS and passes the Fuzzy Parameter Extraction which prepares it for the FIM by comparing, aligning and extracting the network parameters in a way that is most suitable for it. The FIM thoroughly goes through each packet in each node in the traffic and filters and blocks all black hole attacks detected, before allowing the rest of the Network Traffic to proceed to and through the AODV protocol which searches for other security attacks and blocks it. If traces of black hole attack are detected by the FIM, the Black Hole Attack Detection module will signal the Alarm Module to which will be broadcasted to every node in the MANET, of the ongoing attack detection therefore making them more security conscious hence tightening security in general for prevention of further attacks.

4. CONCLUSION

Many solution strategies in security of MANET against black hole attacks have been proposed by researchers, but which solution is the best fit is still up for discussion as attacks and attackers adapt to new security solutions proposed in order to be successful. Hence, this paper proposed an AODV black hole detection model using the Fuzzy Inference System technique in MANET technology. The proposed model modified an already existing model and integrated the FIM into the AODV protocol of the MANET, in order to better its dictation metrics against the Black hole MANET attack. Also, an alarm module was included in the proposed model in order to alert the entire network of possible attack detection and this aids every individual node in the network to suspend activities within the network and implement a temporary possible measure against the present situation of the network.

5. FURTHER STUDY

More research is needed to be done on this idea of using FIM with AODV to detect and block black hole attacks to fine tune the algorithm, develop the proper parameters that the Fuzzy Parameter Extraction will use to accurately prepare the Network Traffic for the FIM by comparing, aligning and extracting the network parameters, in a way that is most suitable for it. Further research is also needed to properly develop suitable algorithms for the module of Black Hole Attack Detection as well as the Alarm Module.

REFERENCES

1. Eze, M., Ajaegbu, C., Maitanmi, O., & Nnakwuzie, D. **A New Alogorithm for Contact Trace Network Evolution and Visualization**. International Journal of Emerging Trends in Engineering Research, vol 8(7), pp. 2934-2939, 2020.
2. Singh, G., Sharma, A. K., Bawa, O. S., & Kaur, H. **Effective Congestion Control in MANET**. Proceedings of International Conference on Intelligent Engineering and Management, ICIEM, pp. 86–90, 2020. https://doi.org/10.1109/ICIEM48762.2020.9160130
3. Prakash, J., Kumar, R., & Saini, J. P. **MANET-internet Integration Architecture**. Journal of Applied Sciences, vol. 17(6), pp. 264–281, 2017. https://doi.org/10.3923/jas.2017.264.281
4. Deng, L., Liu, F., Zhang, Y., & Wong, W. S. **Delay-Constrained Topology-Transparent Distributed Scheduling for MANETs.** pp. 1–17, 2020. http://arxiv.org/abs/2006.07668
5. Ma, D. **MiabNET: Message-in-a-bottle Protocol for MANET**. pp. 2–3, 2020. http://arxiv.org/abs/2008.00083
6. Abdelhaq, M., Alsaqour, R., Alaskar, M., Alotaibi, F., Almutlaq, R., Alghamdi, B., Alhammad, B., Sehaibani, M., & Moyna, D. **The resistance of routing protocols against DDOS attack in MANET**. International Journal of Electrical and Computer Engineering, vol. 10(5), pp. 4844–4852, 2020. https://doi.org/10.11591/ijece.v10i5.pp4844-4852
7. Hrabčák, D., Matis, M., Doboš, L., & Papaj, J. **Students Social Based Mobility Model for MANET-DTN Networks**. Mobile Information Systems, 2017. https://doi.org/10.1155/2017/2714595
8. Zamani, E., & Soltanaghaei, M. **The Improved Overhearing Backup AODV Protocol in MANET**. Journal of Computer Networks and Communications, 2016. https://doi.org/10.1155/2016/6463157
9. Alqarni, B. H., & Almogren, A. S. **Reliable and Energy Efficient Protocol for MANET Multicasting**. Journal of Computer Networks and Communications, 2016. https://doi.org/10.1155/2016/9146168
10. Gandage S.C and Kumar A. **An efficient review of IDS in MANET using PSO**. Journal of Critical Reviews. vol. 7(19). 2020. do**i:** 10.31838/jcr.07.8.548
11. Anjum, S. S., Noor, R. M., & Anisi, M. H. **Review on MANET Based Communication for Search and Rescue Operations**. Wireless Personal Communications, vol. 94(1), pp. 31–52, 2017. https://doi.org/10.1007/s11277-015-3155-y
12. Bruzgiene, R., Narbutaite, L., & Adomkus, T. **MANET Network in Internet of Things System**. Ad Hoc Networks, 2017. https://doi.org/10.5772/66408
13. Cai, R. J., Tan, W. C. W., & Chong, P. H. J. **An Overview of Trust-Based Routing Design Under Adversarial Mobile Ad Hoc Network Environment**. Wireless Personal Communications, vol. 96(3), pp. 3923–3946, 2017. https://doi.org/10.1007/s11277-017-4359-0
14. Fleury, M., Kanellopoulos, D., & Qadri, N. N. **Video streaming over MANETs: An overview of techniques**. Multimedia Tools and Applications, vol. 78, Issue 16, 2019. https://doi.org/10.1007/s11042-019-7679-0
15. Saranya, V., Shankar, S., Nandhini, P., Jayanthi, R., & Cessily, R. J. **Study of various routing protocols in MANETs**. International Journal of Networking and Virtual Organisations, vol. 15(4), pp. 336–358, 2015. https://doi.org/10.1504/IJNVO.2015.073856
16. Jain, A. K., Tokekar, V., & Shrivastava, S. **Security enhancement in MANETs using fuzzy-based trust computation against black hole attacks**. Advances in Intelligent Systems and Computing, vol. 625, pp. 39–47, 2018. https://doi.org/10.1007/978-981-10-5508-9_4
17. Usha, G., Rajesh Babu, M., & Kumar, S. S. **Dynamic anomaly detection using cross layer security in MANET**. Computers and Electrical Engineering, vol. 59, pp. 231–241, 2017. https://doi.org/10.1016/j.compeleceng.2016.12.002
18. Venkatadri, N., & Reddy, K. R. **Secure TORA: Removal of Black Hole Attack Using Two FIMh Algorithm**. Proceedings - 6th International Advanced Computing Conference, IACC, pp. 239–244, 2016. https://doi.org/10.1109/IACC.2016.53
19. Saurabh, V. K., Sharma, R., Itare, R., & Singh, U. **Cluster-based technique for detection and prevention of black-hole attack in MANETs**. Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA, pp. 489–494, January 2017. https://doi.org/10.1109/ICECA.2017.8212712
20. Nitnaware, D., & Thakur, A. **Black hole attack detection and prevention strategy in DYMO for MANET**. 3rd International Conference on Signal Processing and Integrated Networks, SPIN, pp. 279–284, 2016. https://doi.org/10.1109/SPIN.2016.7566704
21. Sathish, M., Arumugam, K., Pari, S. N., & Harikrishnan, V. S. **Detection of single and collaborative black hole attack in MANET**. Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET, pp. 2040–2044, 2016. https://doi.org/10.1109/WiSPNET.2016.7566500
22. Sardana, A., Bedwal, T., Saini, A., & Tayal, R. **Black hole attack's effect mobile ad-hoc networks (MANET)**. Conference Proceeding - 2015 International Conference on Advances in Computer Engineering and Applications, ICACEA, pp. 966–970, 2015. https://doi.org/10.1109/ICACEA.2015.7164846
23. Bhandare, A. S., & Patil, S. B. **Securing MANET against co-operative black hole attack and its performance**

analysis - A case study. Proceedings - 1st International Conference on Computing, Communication, Control and Automation, ICCUBEA, pp. 301–305, 2015. https://doi.org/10.1109/ICCUBEA.2015.63

24. Mejaele, L., & Ochola, E. O. **Analysing the impact of black hole attack on DSR-based MANET: The hidden network destructor**. 2nd International Conference on Information Security and Cyber Forensics, InfoSec, pp. 140–144, 2015. https://doi.org/10.1109/InfoSec.2015.7435519
25. Kumar, R., Quyoom, A., &Gouttam, D. N. **To mitigate black hole attack in AODV**. Proceedings on 2015 1st International Conference on Next Generation Computing Technologies, NGCT, pp. 307–311, September 2015. https://doi.org/10.1109/NGCT.2015.7375131
26. Narang, S. K. **Black Hole Attack Detection using Fuzzy Logic**. International Journal of Science and Research (IJSR), vol. 2(8), pp. 222–225, 2013. https://www.ijsr.net/archive/v2i8/MzAwNzEzMDE=.pdf