JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 07, ISSUE 09, 2020

Protecting Against Black Hole Attacks in Mobile Ad-Hoc Networks Using Energy Routing Protocol

Aditiya Harbola,
Asst. Professor, SOC (School of computing),
GEHU-Dehradun Campus
DOI: 10.48047/jcr.07.09.578

Abstract: Predicting and spotting black hole attacks helps ensure a secure network. Based on the document authority, trust valve, authentication of node, message integrity, and energy level, a new technique of fuzzy inference is proposed for the detection of black hole attacks in this method. The proposed work focuses mostly on node authentication. The fuzzy inference design approach provides better performance on issuing the certificates to the trustworthy nodes exclusively in MANET simulations conducted with the help of the network simulator NS2. As a result, this helps identify and defend against black hole attack-using rogue nodes. Throughput is increased, and End-to-End Delay is decreased, as a result of improvements made to the packet delivery ratio. This demonstrates the system's improved reliability and viability for military use. In order to enable the route discovery process, the initial step of the proposed work primarily focuses on authenticating MANET nodes. Based on factors including node authentication, trust values, certificate authority, energy level, and message integrity, a fuzzy inference method has been developed to identify black hole attacks. newline Mobile Ad hoc Networks (MANETs) provide a formidable challenge for the development of extremely efficient routeing techniques. In order to efficiently react to changes in network topology with little control overhead, minimise packet delay while maintaining a high packet delivery rate, and so on.

Keywords: fuzzy inference design, Mobile Ad hoc Networks (MANETs), overhead, minimise packet delay

Introduction

Nodes in a mobile ad hoc network (MANET) communicate with one another without the need for a master server. It's likely that wireless connections are used by every node in the network to communicate with the others. Due to the fluid nature of a MANET's node design, nodes play a crucial role in maintaining network security. Knowing how to anticipate and identify black hole attacks is crucial for maintaining network safety. Fuzzy inference is presented as a novel approach for detecting black hole attacks, with the proposed criteria including certificate authority, trust valve, node authentication, message integrity, and energy level. The proposed effort is primarily concerned with authenticating nodes. In NS2 MANET simulations, the fuzzy inference design approach improves performance when it comes to just providing certificates to reliable nodes. Therefore, this aids in locating and protecting against black hole attack nodes. Increasing the packet delivery ratio improves throughput and reduces End-to-End Delay. This proves the system's enhanced dependability and military viability. In the first phase of the planned effort, authenticating MANET nodes is prioritised so that routes

may be discovered. Fuzzy inference has been created as a means of detecting black hole attacks based on a number of criteria, such as node authentication, trust values, certificate authority, energy level, and message integrity. Extremely efficient routeing algorithms face a significant problem when used to Mobile Ad hoc Networks (MANETs). With the goal of reducing control overhead, increasing packet delivery rates, and decreasing latency in the face of topology changes. The optimisation problem of secure routeing in MANETs is known to be NP-hard, thus for the time being we'll be focusing on approximation methods. Algorithms that take cues from swarm intelligence (SI) have attracted a lot of attention because to the robustness, adaptability, and low cost they promise. In order to find a happy medium in dynamic MANETs between these competing requirements, the SRACO Meta heuristics for safe routeing has been implemented.

Figure 1 shows a functional MANET in operation. Mobile ad hoc networks are more susceptible to security assaults than cable ones. It is impossible to precisely specify the geographical limits of a mobile ad hoc network. In a nomadic setting, nodes may freely join or leave a wireless network. When an opponent comes within radio range, it will automatically link up with a node. Nodes in a MANET are free to come and go as they like. The network's nodes may exhibit malicious behaviour, but determining whether or not a particular node's actions were malevolent could be challenging.

A more perilous attack than one from the outside. These hosts have been marked as "compromised" because they have been infected with malware. Without a centralised command and control structure, MANETs provide a number of potential security risks. This makes it harder to see any potential assaults as they happen. Centralised monitoring of traffic cannot be performed at the level of individual nodes. If the advisor changes the assault pattern and the attack target, it will be harder to spot an attack. The problem might have been caused by an attacker or a network error. We are unable to label the nodes as trustworthy or untrusted since there is no security relationship between them. All the nodes in a Mobile Ad hoc Network run on battery life. The assumption here is that other power sources are unavailable. The adversary is able to flood the target with traffic.

Continuously processing these packets might drain the target node's battery life. Therefore, the node will be unable to provide its usual network functions. Sometimes, attackers may trick nodes into doing a lengthy calculation that does nothing except drain their batteries. Selfish nodes might exist in a network. A node that lacks cooperation does not work together while performing a common algorithm. Cluster-based intrusion detection systems, for instance, use a network's nodes in concert to spot malicious activity. A node that volunteers to act as a monitor is chosen using the monitor selection method. A harmful act may escape becoming the monitor by opting out of it. Selfishness will lead to the breakdown of the whole system. Mobile ad hoc network scalability is evolving in real time. The predicted number of nodes in mobile ad hoc networks in the future is very speculative. Adapting the protocols and services of MANETs to this new scale is essential.

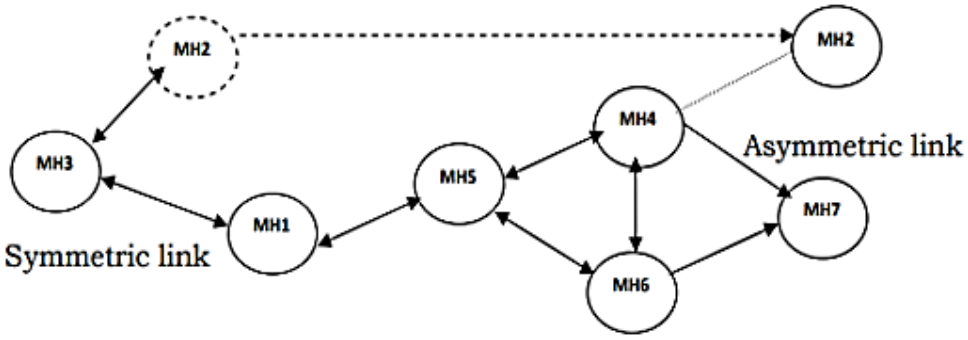

Figure 1. Mobile Ad hoc Networks

Topology Management

Topology management, which takes into account both the physical and logical connections between nodes, is crucial to MANETs' network administration. Topology control is the primary focus for conserving power when online. The following are some goals that may be accomplished by topology management: The network's nodes' transmitted power may be adjusted to give a select few subbranches more say in network operations. By grouping or clustering nodes together, energy consumption may be reduced. Establishing links to neighbouring clusters by picking escape nodes. Active control of MANET architecture is possible via the modification of the nodes' transmission power. This is why transmission power management is a common name for the topology control method used in MANETs. Transmit power management is a physical layer approach that regulates the amount of signal strength sent from a transmitter to a receiver. Topology management aims to reduce power consumption, which is particularly important in MANETs. Other objectives include reducing latency and increasing throughput. More power is used by the MANET's radio circuit than by any other part of the computation. Despite this, MANETs that use multi-hop communication lead to higher radio power consumption and interference signals. When the transmission range of a network is too little, a sparse topology might cause communication breakdown. It's also not ideal to provide each node an excessive amount of electricity to transmit with. As a result, MANET neighbour selection is intricately tied to the neighbor-based power control mechanism. Assigning appropriate transmission ranges to the nodes is essential for minimising resource drain and noise interference while keeping the network operational. These algorithms' overarching goal is to improve communication performance, network reliability, and power efficiency. Currently, most approaches to controlling the network's topology are reactive, meaning they aim to make changes to the topology only after a link change has already happened. To overcome this limitation, researchers are focusing on proactive topology control algorithms or predictive algorithms that modify the transmission powers of communication nodes.

The initial step in route discovery in mobile ad hoc networks is authenticating the nodes in the network. The fuzzy inference system may be able to detect a black hole attack by analysing factors including node authentication, trust values, certificate authority, energy level, and message integrity. To improve the system's speed, which is further improved by

fuzzy criteria, certificates are issued to only trustworthy nodes. This might lead to the discovery of harmful nodes and the avoidance of black holes. Secured routeing in MANETs is an NP-hard problem, and this level looks at approximate solutions to this problem. Swarm Intelligence (SI) algorithms have garnered a lot of attention because of their potential to provide robust, versatile, and cost-effective solutions. The meta heuristic Ant Colony Optimisation (ACO) has been successfully applied to dynamic MANETs. In the last phase, an optimal routeing strategy for wireless mobile networks will be shown. The black hole attack may be avoided thanks to this trust model, which employs a Differential Evolution technique to detect hostile nodes and bar them from joining the data transmission channel.

Literature Review

Sharma Hitesh Omprakash et.al.,(2020) In this study, we introduce two attacks that have a negative impact on network performance—the Black hole Attack and the Grey hole Attack—and apply them to a realistic network situation characterised by the random mobility of nodes. Our study uncovered an innovative method of defence that successfully defends against network-based attacks and their secondary effects.

Ephantus Gichuki et.al.,(2019) This study examines the efficacy of many anti-black hole attack security approaches and routeing procedures. Using the stated knowledge gaps as a starting point, we will create a security method that can withstand collaborative black hole assaults.

Lokesh Baghel et.al.,(2017) The security of mobile ad hoc networks (MANET) is crucial. Researchers are working hard on every aspect of MANET security to protect the networks from rogue nodes. Secure routeing systems have been proposed using several novel methods for use in wireless networks The experimental results demonstrate the superiority of the proposed method over the gold standard AODV.

Detection and Prevention of Black Hole Attack Using Fuzzy Heuristics

There is no dependable backup server for the distributed machines in a MANET. To communicate with other nodes in the network, each one is equipped with its own wireless connection. Because of the fluid nature of a MANET, the nodes within it play a crucial role in maintaining network safety. Knowing how to anticipate and identify black hole attacks is crucial for maintaining network safety. In this approach, a novel method of fuzzy inference is presented for identifying signs of black hole attacks by combining the certificate of power, trust valve, authentication of nodes, message integrity, and energy level. Authentication of nodes is a primary focus of the proposed effort. As shown in simulations run with the aid of network simulator NS2, the fuzzy infer design method improves the efficiency of MANET when it comes to providing certificates to the reliable nodes. In mobile ad hoc networks, the proposed work focuses on authenticating nodes before starting the route finding process. Using factors including node authentication, trust values, certificate authority, energy level, and message integrity, a fuzzy inference method has been developed to identify a black hole attack. The system's efficiency is enhanced by fuzzy rules, which restrict certificate issuance to verified nodes.

Node Authentication using Fuzzy based Analyser

When trust values show a constructive direction, reliable nodes rise in number, whereas when trust levels show a pessimistic worry, reliable nodes decrease. The trust levels in fuzzy logic might be anything from 0 to 1.

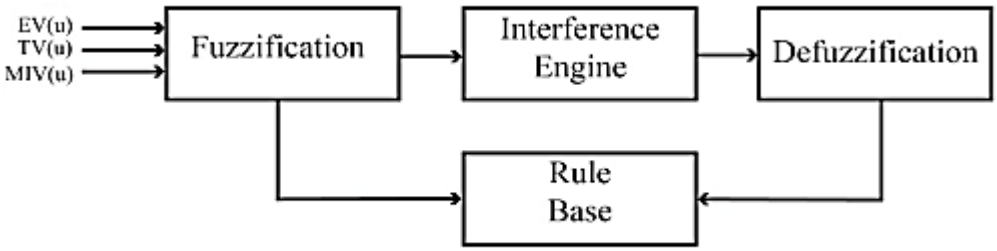

Figure 2. Fuzzy design approach

Figure 2 depicts the fuzzy approach structure of the suggested system, which has four inputs and one output. Node u's Direct Trust (DT(u)), Energy Value (EV(u)), Trust Value (TV(u)), and Message Integrity Value (MIV(u)) are all inputs to the fuzzification method, while the defuzzification-enabled Node type (crisp) is the resulting output.

With the fuzzification technique in mind, the inference engine receives crisp inputs and converts them into fuzzy trust values. The rule base stores the network constraints that inform the inference engine's several techniques for enabling outcomes. Certificate Authority will only give a certificate to the node with the highest f(u) value, which is determined by the ruleset. When everything else fails, the chosen node takes over as the forwarder in the chain. Very Low (VL), Low (L), Medium (M), High (H), and Very High (VH) are the five levels of membership functions used to calculate N(u).

Fuzzy Level	Trust Value	Output
		Normal (Trusted) / Malicious
Very Low	0 to 0.2	Malicious
Low	0.2 to 0.4	Malicious
Medium	0.4 to 0.6	Trusted
High	0.6 to 0.8	Trusted
Very high	0.8 to 1	Trusted

Table 1 Fuzzy discrimination

The simulation is done through the NS-2, with varying network speed. The Table 3.2 represents the network scenario for simulation.

Table 2 Simulation parameters

Parameters	Value
Area	1000 m^2
Routing Protocol	AODV
Data rate	5 pks/s
Packet Size	64 bytes
Number of nodes	20, 30, 40, 50
Simulation time	600ms
Traffic model	CBR
Transmission Range	250m
Node speed	2 ms
Pause time	10s

Results and Analysis

The performance of Certificate Authority with Fuzzy Approach was evaluated and compared with AODV with Black Hole Attack and Normal AODV depends on Packet Delivery Ratio, throughput, Detection Ratio of Malicious Node, and the End-to-End Delay. The performance analysis describes the number of nodes were clustered as 20, 30, 40, 50, 60 and the malicious nodes as 5, 10, 15, 20 and 25 respectively.

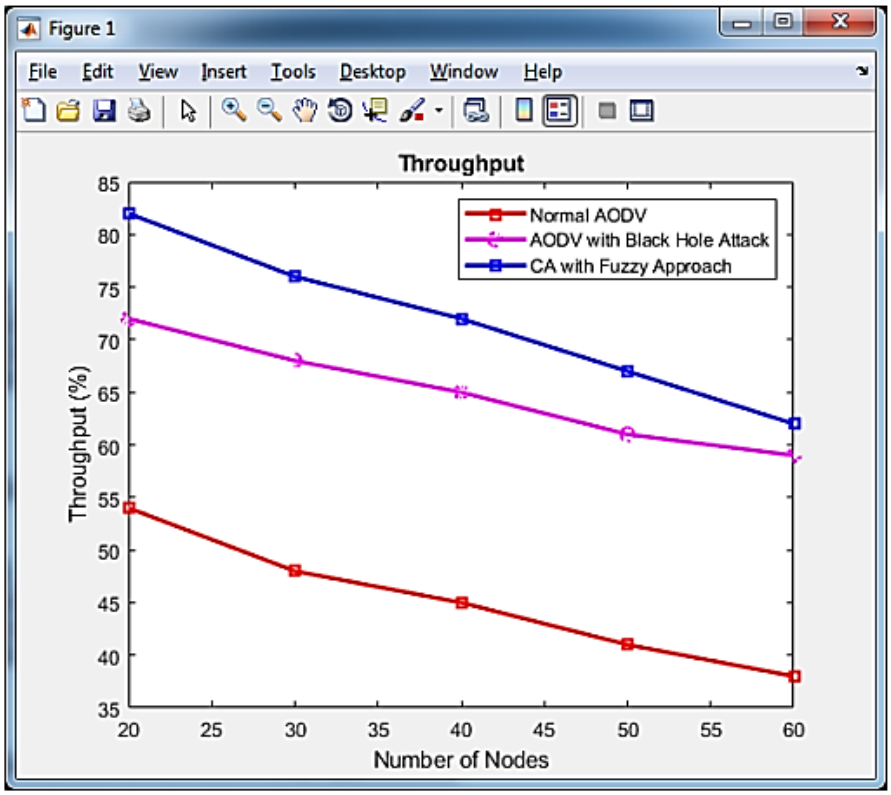

Figure 3. Throughput performance comparison

Figure 3. shows the proposed method performance CA with Fuzzy approach. From the figure one can observe that the maximum throughput 84% is given by CA with Fuzzy Approach when the number of nodes is 20.

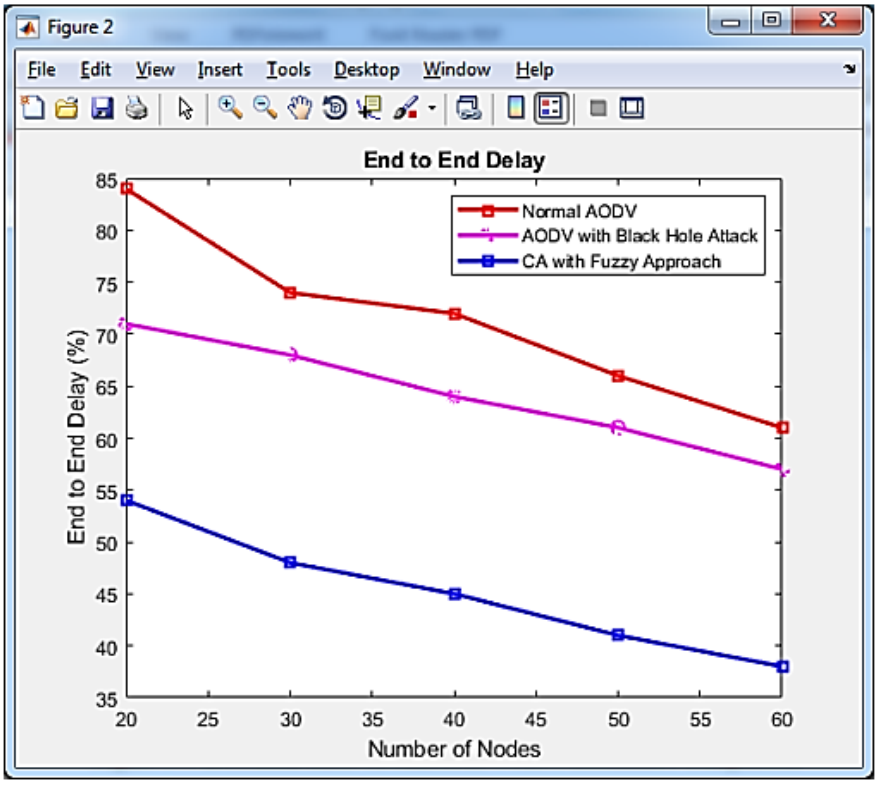

Figure 4. End to End delay performance comparison

Figure 4 illustrates the proposed method performance CA with Fuzzy approach. From the figure one can observed as 38% of End-to-End delay CA with Fuzzy Approach when the number of node is 60.

Conclusion

Based on the node's authentication, Certificate Authority, message integrity, energy level, and trust value, a fuzzy inference system may identify a black hole attack. The proposed approach focuses primarily on authenticating nodes prior to starting the route discovery process in MANETs that are used to counteract the black hole attack. When only trustworthy nodes in a fuzzy inference system are given certificates, the system performs much better. The proposed Certificate Authority with Fuzzy Approach outperformed state-of-the-art methods like AODV and Normal AODV with Black Hole Attack in terms of End-to-End Delay, throughput, Detection Ratio of Malicious Node, and Packet Delivery Ratio. The suggested technique successfully detects and isolates black hole attacks in mobile ad hoc networks, as shown by the findings and comparisons. Since increasing the number of nodes beyond 60 would provide more consistent findings, we are constrained to using no more than 60 in our experiments.

References

1. S. H. Omprakash and M. K. Suthar, "Mitigation Technique for Black hole Attack in Mobile Ad hoc Network," *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, 2020, pp. 1-5, doi: 10.1109/ICCCNT49239.2020.9225381.
2. E. G. Mwangi, G. M. Muketha And G. K. Ndungu, "A Review of Security Techniques against Black hole Attacks in Mobile Ad hoc Networks," *2019 IST-Africa Week Conference (IST-Africa)*, Nairobi, Kenya, 2019, pp. 1-8, doi: 10.23919/ISTAFRICA.2019.8764862.
3. L. Baghel, P. Mishra, M. Samvatsar and U. Singh, "Detection of black hole attack in mobile ad hoc network using adaptive approach," *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 2017, pp. 626-630, doi: 10.1109/ICECA.2017.8212741.
4. D. Khan and M. Jamil, "Study of detecting and overcoming black hole attacks in MANET: A review," *2017 International Symposium on Wireless Systems and Networks (ISWSN)*, Lahore, Pakistan, 2017, pp. 1-4, doi: 10.1109/ISWSN.2017.8250039.
5. M. Mistry, P. Tandel and V. Reshamwala, "Mitigating techniques of black hole attack in MANET: A review," *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, Tirunelveli, India, 2017, pp. 554-557, doi: 10.1109/ICOEI.2017.8300721.
6. J. V. Vadavi and A. G. Sugavi, "Detection of black hole attack in enhanced AODV protocol," *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, Gurgaon, India, 2017, pp. 118-123, doi: 10.1109/IC3TSN.2017.8284462.
7. S. Gurung and S. Chauhan, "A review of black-hole attack mitigation techniques and its drawbacks in Mobile Ad-hoc Network," *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2017, pp. 2379-2385, doi: 10.1109/WiSPNET.2017.8300186.

8. R. S. Abdullah and S. Hariganesh, "OTPR - Optimum Transmission Power Routing against Black Hole Attacks in MANETs," *2017 World Congress on Computing and Communication Technologies (WCCCT)*, Tiruchirappalli, India, 2017, pp. 47-50, doi: 10.1109/WCCCT.2016.21.
9. V. Trivedi and V. Preethi, "Depictive Analysis of MANETs under Black Hole Attack," *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, Mysore, India, 2017, pp. 1116-1120, doi: 10.1109/CTCEEC.2017.8455010.
10. A. Kumar Jain and A. Choorasiya, "Security enhancement of AODV routing protocol in mobile ad hoc network," *2017 2nd International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, 2017, pp. 958-964, doi: 10.1109/CESYS.2017.8321223.
11. A. Sardana, T. Bedwal, A. Saini and R. Tayal, "Black hole attack's effect mobile ad-hoc networks (MANET)," *2015 International Conference on Advances in Computer Engineering and Applications*, Ghaziabad, India, 2015, pp. 966-970, doi: 10.1109/ICACEA.2015.7164846.
12. A. K. Jain and V. Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks," *2015 International Conference on Pervasive Computing (ICPC)*, Pune, India, 2015, pp. 1-6, doi: 10.1109/PERVASIVE.2015.7087174.
13. A. Jain and A. Shrotriya, "Investigating the effects of black hole attack in MANET under shadowing model with different traffic conditions," *2015 International Conference on Computer, Communication and Control (IC4)*, Indore, India, 2015, pp. 1-6, doi: 10.1109/IC4.2015.7375590.
14. N. Arya, U. Singh and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," *2015 International Conference on Computer, Communication and Control (IC4)*, Indore, India, 2015, pp. 1-5, doi: 10.1109/IC4.2015.7375649.
15. S. V. Vasantha and A. Damodaram, "Bulwark AODV against Black hole and Gray hole attacks in MANET," *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Madurai, India, 2015, pp. 1-5, doi: 10.1109/ICCIC.2015.7435734.
16. N. Choudhary and L. Tharani, "Preventing Black Hole Attack in AODV using timer-based detection mechanism," *2015 International Conference on Signal Processing and Communication Engineering Systems*, Guntur, India, 2015, pp. 1-4, doi: 10.1109/SPACES.2015.7058198.