DETECTION OF SYBIL ATTACK IN MANET ENVIRONMENT USING ANFIS WITH BLOOM FILTER ALGORITHM

Dr. Pinagadi Venkateswara Rao

Associate Professor, Department of CSE, ACE Engineering College, Ghatkesar, Hyderabad, India
venkat.pinagadi@gmail.com

Dr. K. Sreerama Murthy

Associate Professor, Department of IT, Sreenidhi Institute of Science & Technology, Ghatkesar,
Hyderabad, India
sreeram1203@gmail.com

Dr. V. Gokula Krishnan

Associate Professor, Department of CSIT, CVR College of Engineering, Mangalpally, Hyderabad, India
gokul_kris143@yahoo.com

V. Divya

PhD Research Scholar, School of Electrical and Electronics Engineering, Sathyabama Institute of Science and
Technology, Chennai, Tamil Nadu, India
vdivya6891@gmail.com

K. Sathyamoorthy

Assistant Professor, CSE Department, Panimalar Institute of Technology, Chennai, Tamil Nadu, India
pitsathyamoorthy@gmail.com

Abstract

MANET is a temporary network that is dynamically constructed from a gathering of mobile nodes. It runs completely independently of any preexisting infrastructure. Self-deliberate networks, in which every network point acts as a source or router, let nodes to freely move around the network. MANET is critical in a system without a link. Mobile ad hoc networks require a high level of security to protect sensitive data from being accessed by unauthorized parties. Routing protocol assaults are the most common type of attack in MANET. The goal of the current study is to identify and prevent a Sybil assault on the network. One of MANET's well-known security threats is the Sybil attack. Malicious nodes draw the data packet by addressing a bogus path, resulting in a Sybil attack. To detect Sybil attacks in MANET, this research proposes an adaptive network-based fuzzy inference system (ANFIS) with a Bloom Filter. If a source node wants to connect with a destination via this approach, it relies on the observing nodes to altercation details such as distance, angle, and RSSI (Received Signal Strength Indicator) difference with the two-hop neighbor nodes collectively. Fuzzy logic decision with Bloom Filter is used to discover the suspected Sybil attack nodes based on the acquired information. Since an exchange of monitoring nodes has validated the Sybil assault, there is a reduced probability of false and missed detection. Packet delivery ratio (PDR), latency, energy usage, and overhead have all been considered when evaluating system performance. The NS-2 simulator tool was used to run the simulations.

Keywords: **Bloom Filter; Security; Mobile Adhoc Network; Fuzzy Logic; Sybil Attack; Received Signal Strength.**

1. Introduction

In the wireless networks, mobility and scalability have been provided by moved the people from the wired network into a wireless network. In general, the Wireless networks contain two categories, one is the infrastructure category and another one is ad-hoc networks. In infrastructure- based networks, the data transmission will happen between the access points and the wireless node, other than communication does not occur directly between the wireless nodes. When the access point cannot be synchronized, the Collisions may have happened in an infrastructure network. For disaster relief, they will be exploited in cases where ever no infrastructure can be obtainable. In the Ad hoc network, any network infrastructure is not needed for the data communication process. Every mobile node will transfer the data directly with other mobile nodes, thus no access point can be required in the Ad hoc network.

MANET can be acted as the self-configuring network with connected mobile nodes by using the wireless links and it is measured as an Ad hoc network without the utilization of infrastructure. The wireless mobile odes have been grouped in the MANET, in which every mobile node was equipped with both a transmitter and a receiver. The wireless mobile nodes may be in the form of PDAs (Personal Digital Assistants), mobile phones, laptops, etc. In this kind of network, the individual mobile node can be assisted by forwarding the packets to each other while the destination node packets are ahead of the wireless transmission range of source mobile node. The MANET topology is dynamic by nature, as nodes are always moving. There are unique challenges when building routing protocols for this form of network because of the mobile nature of nodes [1]. These factors include restricted bandwidth, high error rates, and low battery power. Mobile ad hoc networks have unique characteristics, such as resource-constrained devices and changing topology that make designing security protocols more difficult [3]. The path prediction is unclear because of the mobile nodes' dynamic nature. If the nodes comply with the forwarding activities, they are labeled as well-behaved; otherwise, they are labeled as misbehaving nodes. The nodes are also divided into three categories: defective nodes, selfish nodes, and malign nodes. Due to hardware and software errors, faulty nodes do not collaborate. Selfish nodes employ other nodes to forward packets they receive from the sender node. Malicious nodes slow down packet delivery and cause havoc on the MANET's normal operation.

MANETs, like other radio-based media systems, are subject to numerous dangers. These threats include both outside assailants and inside wayward items. There are therefore numerous pledge technologies that must be installed in order to safeguard these kinds of systems as data protection management [4-5]. Researchers have found a slew of ramifications for wireless networks and the independence of their various apparatus when employing well-established intrusion-detection techniques and applications that aren't immediately invisible from infrastructure-based IP address networks [6]. Even if the strike for smart and broadband continues, the risk of spoofing and Man in the Middle attacks within the system has also increased. Due to the possibility of protocol packs not being transported effectively, false alarms and unfounded accusations against nodes from the networks are relatively common [7]. As long as you're in the system, this potential gets better with movement. It is also true that in wired IP networks, such as switches, routers, and firewalls, all appropriate visitors could be recognized and evaluated in order to uncover harmful activities [8].

Sybil attacks pose a severe danger to MANET networks because of the lack of centralized identity management in the network, which necessitates different, permanent identities and unique per node [9].

1.1. Sybil Attack Detection in MANET

There is no central authority or management for preserving the MANET network, making it more vulnerable to numerous attacks. The Sybil assault is widely acknowledged as the primary factor in the network's demise [10]. Wireless sensor networks (WSN) and MANET have been subject to the Sybil assault, which is one of the most damaging. The Sybil attack occurs when a malicious node exploits the identities of numerous phonies illegally to confuse and collapse the network. A sybil assault can occur both internally and externally to a system. An authentication method can stop external assaults like the Sybil node trying to get into the network, but it cannot stop attacks from within the network. In order for each node to establish its integrity, the authentication mechanism assures that there should be a mapping between the entity and individuality in the network. By creating many false identities for the same node, this attack also breaks the one-to-one correspondence. There are numerous risks associated with Sybil attacks. These include the development of extreme hazard in routing protocols as well as fair resource allocation and online voting systems.

1.2 Characteristics of MANET

The Characteristics of MANET are listed below:

- **Dynamic Topologies:** In MANET, the network topology that can be characteristically multi-hop, and it can be changed arbitrarily and quickly at a time, it will outline the bi-directional or unidirectional links. The throughput of this network can be even less than a maximum transmission rate of the radio subsequent for dealing with the restrictions such as noise, multiple access, intrusion situations, etc.
- **Less Human Involvement:** The MANET is needed in the smallest amount of human involvement to organize the network; as a result, they can be enthusiastically self-directed in character.
- **Variable capability, bandwidth constrained links:** The wireless links of MANET typically contain effectiveness, lesser dependability, constancy and capability than the wired network.
- **Energy Controlled Procedure:** For the energy, every mobile node is worked according to the batteries or other exhaustible. In MANET, every mobile node has been distinguished in terms of power, less memory, and light weight characteristics.
- **Self-governing Performance:** Every mobile node in MANET can be acted as a router and host and this has shown its self-governing performance.

- **Inadequate Security:** MANETs can be additional prone to security attacks. A central firewall is not present during its disseminated nature of the process for security, host configuration and routing.

The deployment of an Intrusion Detection System (IDS) is critical in MANET security to thwart such an assault. The objective of the study is to detect the Sybil attack in MANET network by introducing the intrusion detection technique using ANFIS with bloom filter technique. The related work is accessible in Section 2, the brief explanation of the proposed technique is provided in Section 3. The validation of proposed method with existing techniques in terms of attacks is presented in Section 4. Finally, the scientific contribution of research work with future development is described in Section 5.

2. Related Works

Based on an optimization approach, Veeraiah and Krishna [12] propose a powerful MANET multipath routing protocol. As a result of the cluster head's gathering and intrusion mitigation procedures, the MANET energy and protection crisis can be effectively addressed (fuzzy NB). This approach incorporates bird swarm optimization (BSA) into the whale optimization algorithm, which is subsequently used to advance the multipath routing according to the routing protocol (WOA). It was suggested by Prasad and Shankar [13] that the EA-DRP protocol be adopted with changes to the current DSR and that the proposed protocol's total energy usage be lowered. EA-DRP algorithm reduces network energy use by an impressive amount. Because of its low power consumption, the EA-DRP is well suited for enhancing wireless communication and locating alternate pathways between mobile nodes in a network. For various sorts of attacks, the performance of this approach is poor.

Energy Efficient EE-OHRA route discovery for MANET was proposed by Vinod Kumar and Anuratha [14] as a version aimed at addressing difficulties associated with minimizing energy consumption and maximizing course life. When using our suggested strategy for discovering new courses, we consider the course's remaining lifespan, since the metric shrinks with each subsequent choice. Because there are fewer ways to discover routes now, the routing protocol runs faster because the overhead calculation on all nodes involved is reduced. The method's performance varies greatly depending on the sort of attack. There are two authors: Borkar and Mahajan. The proposed method necessitates an adaptive strategy that improves our scheme's energy efficiency. With the filtering approach, a node's per-unit-time RREQ generation spreads more slowly, which reduces interference. Successful denial-of-service attacks The AODV routing protocol's security was bolstered by this study's multipath extensions and security enhancements.

As part of the AODV routing protocol, the hash function with location update algorithm is proposed by Taha et al. Data packets are relayed via the AODV routing protocol from the source to the target location. For this reason, the Prevention of Selfish Node using Hash Function (PSNHF) with location update technique is recommended to minimize packet loss across the network. In order to efficiently communicate data, a new QoS based protected multi-path routing architecture is suggested by Kavuru Tejaswi Uttej Kumar et al. [17]. Additionally, the multipath routing phase uses the AODVBR protocol and Optimal Fuzzy Logic. Grey Wolf Optimization Adaptive Formation anticipates the best-case scenario. Homomorphic Encryption is used to protect data key management procedures by selecting an optimum route from the known routes. The productivity of the planned methodology is assessed using metrics such as end-to-end latency, packet distribution ratio, and so on.

Mallikarjuna et al., [18] propose a solution called dependable and secure multipath routing for MANETs with congestion perception. While routing, this strategy's primary focus is on increasing bandwidth while also minimizing latency. Networks can evaluate their own residual energy and dependability using this method. When determining the remaining energy, it also takes into account the node's receiving and transmitting energy. When the LET connection has been determined to be stable, motion parameters are used to acquire it. Using these factors, the network determines the best path to use for relaying data packets between nodes.

According to Rajashanthi and Valarmathi [19], secure multi-path routing and data transmission can be achieved by utilizing digital signatures to sign RREQ packets for route finding. At this point, the source node session key is checking all of the destination's signatures and the path list is stored in the destination's cache. The RREP is then sent in the same direction back to the originating node. The route is approved if the signature has been verified. Session keys and the hash function are used to encrypt the message components at the source node. Depending on the nodes' confidence, safe routing can be established. An algorithm was utilized to find the safest possible route. In order to decrypt the data, it is first split into four bits, encrypted, and then subjected to XOR procedures. In the end, the target node recovers the original message after it has been decrypted and restored.

3. Proposed Intrusion Detection System

For the identification of sybil attacks, many research have used the fuzzy inference system (FIS), which relies on humans' knowledge to choose the number of membership functions for each fuzzy set, as well as its location and shape. Because of this, they come up with fuzzy rules. As a result, even with a highly skilled researcher, optimizing these characteristics is tough. In order to construct fuzzy rules and membership functions automatically, a well-optimized system is required. To detect the Sybil attack, this study proposes an intrusion detection system that utilizes a combination of ANFIS and Bloom Filter. By modifying the membership functions and decreasing error, the bloom filter improves ANFIS performance in this new IDS. As a result of the ANFIS predictions, the attacker's future behavior can be reconstructed and detected.

3.1. Adaptive neuro fuzzy inference system

Fuzzy logic is included into neural networks using ANFIS [20]. Hybrid learning is used in this model to simulate the relationship between a process' input and output in order to figure out the best way to distribute membership functions. It is based on Takagi and Sugeno's "if... then" rules. Each of the model's five layers, which have multiple nodes, is organized as follows: (see Fig. 1). The adaptive square nodes have parameters, whereas the fixed circular nodes do not. As an illustration, consider two input variables x 1 and x 2, each with two linguistic terms describing it: M1 and M2 for x 1, and L 1 and L 2 for x 2, respectively. As a result, a rule base "if... then" is defined by two fuzzy rules R 1 and R 2:

R_1: if x1 is M_1 and x_2 is L_1 then $y = f_1(x)$

R_2 : if x1 is M_2 and x_2 is L_2 then $y = f_2(x)$

$$f_1(x) = p_1x_1 + q_1x_2 + r_1$$

$$f_2(x) = p_2x_1 + q_2x_2 + r_2$$

The conclusion part's parameters are represented as p_i, q_i and r_i which will be changed during training.

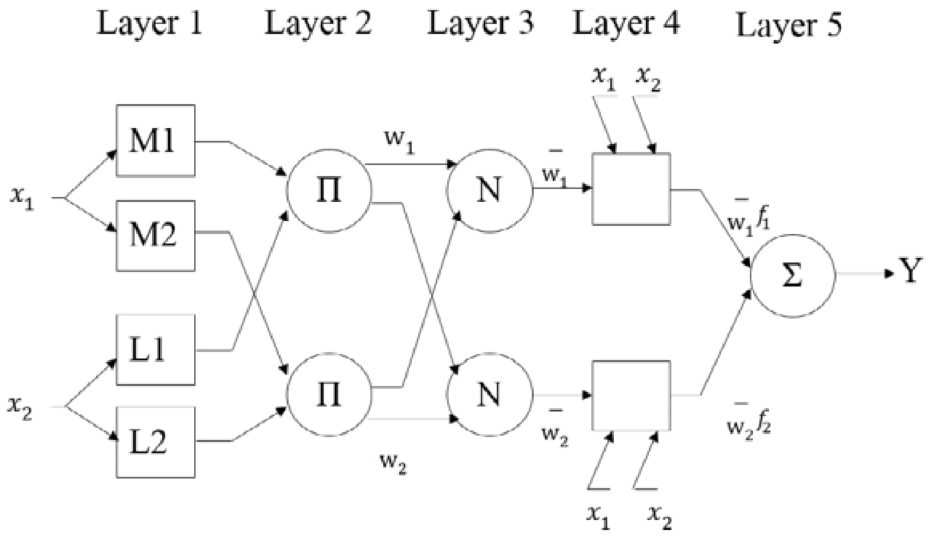


Fig. 1. Architecture of ANFIS algorithm.

In order to improve the performance of the ANFIS, bloom filter is applied in this technique and then, it will detect whether a node is attacked by Sybil or not.

3.2. The Bloom filter

The Bloom filter is a probabilistic data structure that saves on storage space by determining whether or not a node or object belongs to a given subset. A Bloom filter represents a vector of m bits that describes the set $S = s1, s2, \ldots, sn$ for n elements. All values are initially set to 0 (zero). To generate a random integer between 1 and m, the filter employs the hash functions $h1, h2, \ldots, hk$. The Bloom filter serves as an authentication technique for source node packets in our design. A source node builds a Bloom filter output from packets sent as part of a flow it originated and delivers it to its contacts whenever packets are sent as part of that flow. Authentication for packets created by a given source is provided by the Bloom filter output. Each intermediate node sends the signed filter output associated with the packets it receives from a certain flow to its contact in order to perform packet-level authentication on all of the intermediate nodes. Figure 2 shows the bloom filtering process.

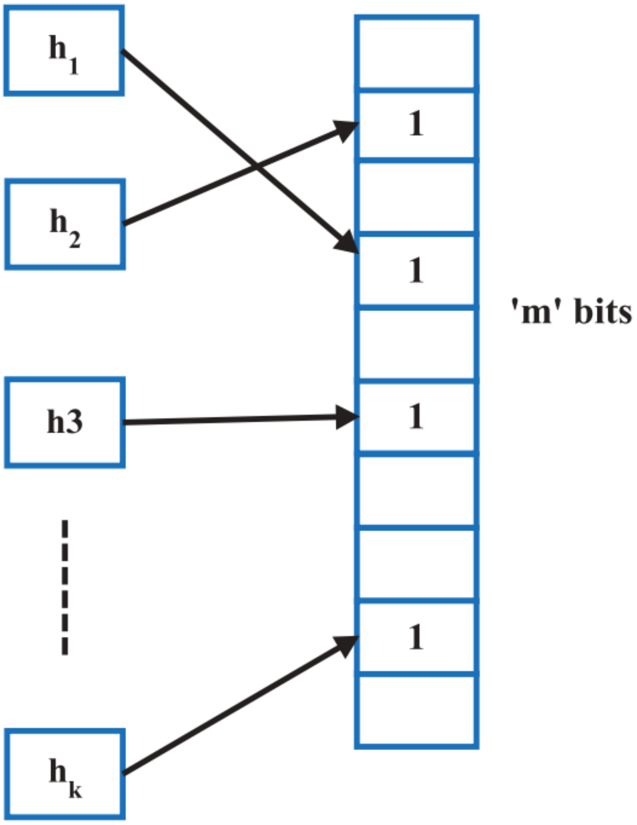
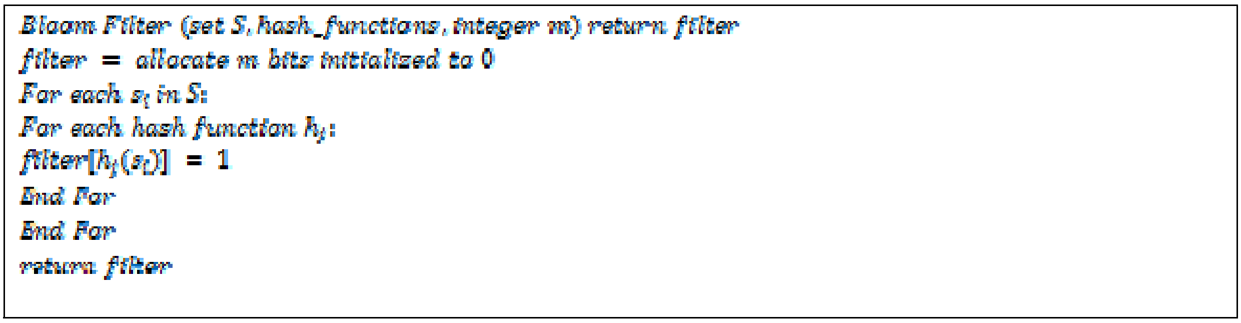


Fig.2. Bloom filtering process.

Consider a set $S = \{s_1, s_2, \ldots, s_n\}$ of n elements. The Bloom filter describes the membership info of S using a bit vector V of length m. The subsequent process builds an m-bit Bloom filter, consistent to the set S and using $h_1, h_2, \ldots, h_k$ hash functions. Initially, the m-bit array is filled with zeros. Each item in the set is hashed for k times. If the hash value of the item is equal to a, then B[a] is set to 1.

3.2.1. Bloom filter algorithm



```
Bloom Filter (set S, hash_functions, integer m) return filter
filter = allocate m bits initialized to 0
For each $s_i$ in S:
For each hash function $h_j$:
filter[$h_j(s_i)$] = 1
End For
End For
return filter
```

A Bloom filter is used to monitor the sybil attacks. The main objective is to record the incoming session and information used during the detection process. It uses a single memory solution to indicate an attack and monitored information to identify the malicious messages. Hence, the Bloom filter is considered as an efficient and affordable technique for recording a huge amount of monitoring information in a compact data storage.
This stage involves two main procedures

- Transmission of node identity (ID) for authentication
- Using ID to detect attacks

3.2.2. Transmission of node ID

The neighboring nodes send their identities $\{ID_1, ID_2, \ldots, ID_n\}$ upon receiving the hello packet broadcast from the source node. The hash function of the ID is created as Hash (ID_i). The source node acquires the IDs of the neighboring nodes and registers the IDs. The hash value of the node ID is created by using the Authentication Identity Filtration (AIF) and authenticated data is generated. To prevent hacking of the authenticated data, the source node encrypts the authenticated data using a secret sharing scheme and generates encrypted data packets called shares.

Upon receiving the originating node's greeting packet broadcast, the adjacent nodes communicate their IDs, $\{ID_1, ID_2, \ldots, ID_n\}$. Hash ($ID_i$). is used to build the ID's hash function. As the nearby nodes acquire and register their IDs, the source node keeps track of theirs. Authenticated data is derived from the hash value of the node ID using Authentication Identity Filtration (AIF). A secret sharing mechanism used by the source node encrypts authenticated data, making it impossible to steal, and then generates encrypted data packets known as shares as a result of that encryption.

3.2.3. Attack detection using node ID

The destination node evaluates the secret shares and detects the presence of attacks. It decrypts the AIF using the received secret shares. The destination node compares the decrypted AIF with the hash AIF. If the two values are identical, the endpoint node judges the decrypted AIF as legitimate. Otherwise, the destination node judges that the received AIF is an attack and discards it.

The Bloom Filter technique is used to update the initial values of the premise and subsequent parameters in the ANFIS model. To put it another way, Bloom Filter will identify the best starting point and all the criteria that follow. ANFIS then uses these optimized parameters to get the final result that is in line with our predictions.

4. Results and Discussion

In order to test our ideas, we ran them through a computer simulation called NS-2. IEEE 802.11 is the MAC protocol used by the networks. This functionality notifies you if a network layer link has broken. Based on the results of the simulation, the node count can range from 20 to 100. The square region's size is 5050 m for a 50 s simulation. Simulated traffic is defined as having a constant bit rate (CBR). The simulation settings and parameters are summarized in Table 1, which follows.

Table 1. Simulation Constraints

Simulator	NS-2
Simulation time	50s
Transmission power	0.3
Initial energy	10.1 J
Receiving power	0.3
Number of mobile nodes	100
Area	50×50
Propagation	Two ray ground
Traffic source	CBR (constant bit rate)
MAC	802.11
Flows	2, 4, 6, 8 and 10
Antenna	Omni antenna

4.2. Performance Analysis of Proposed Model

In this section, the validation of proposed model (ANFIS-Bloom Filter) is analyzed with existing techniques such as ANFIS with Genetic Algorithm (GA) and ANFIS with Particle Swarm Optimization (PSO) in terms of various metrics. Initially, these performances are tested using delay versus attacks, which is shown in Figure 3.

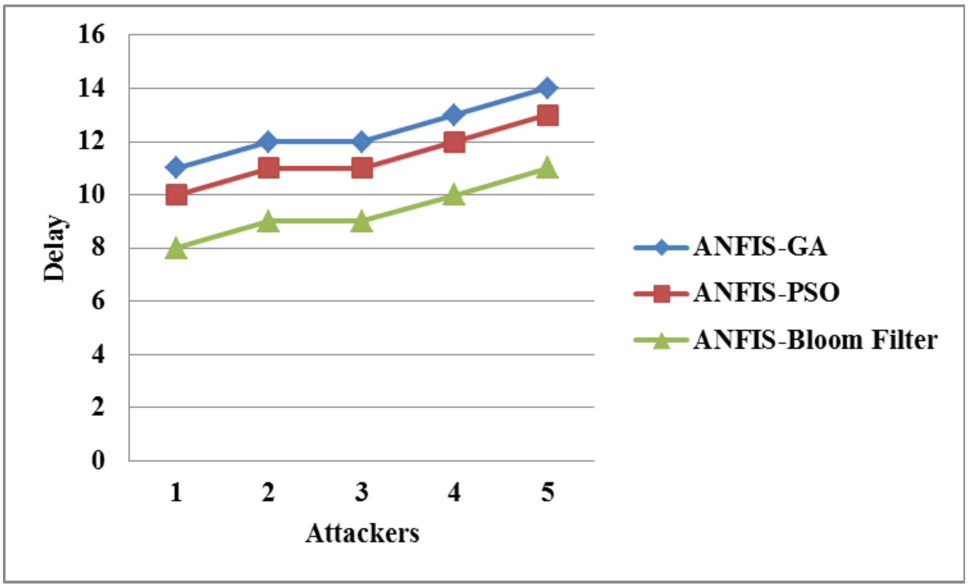


Fig. 3. Validation of Proposed ANFIS-Bloom Filter with respects to Attackers versus delay

When the attackers are increased, the delay for each technique's is also increased. For instance, ANFIS-GA achieved 11sec of delay, ANFIS-PSO achieved 10sec of delay and proposed method achieved 8sec of delay, when the attacker is 1. However, these techniques achieved 14sec, 13sec and 11sec of delay when the attacker reaches 5. Figure 4 shows the graphical representation of proposed model in terms of Packet Delivery Ratio (PDR).

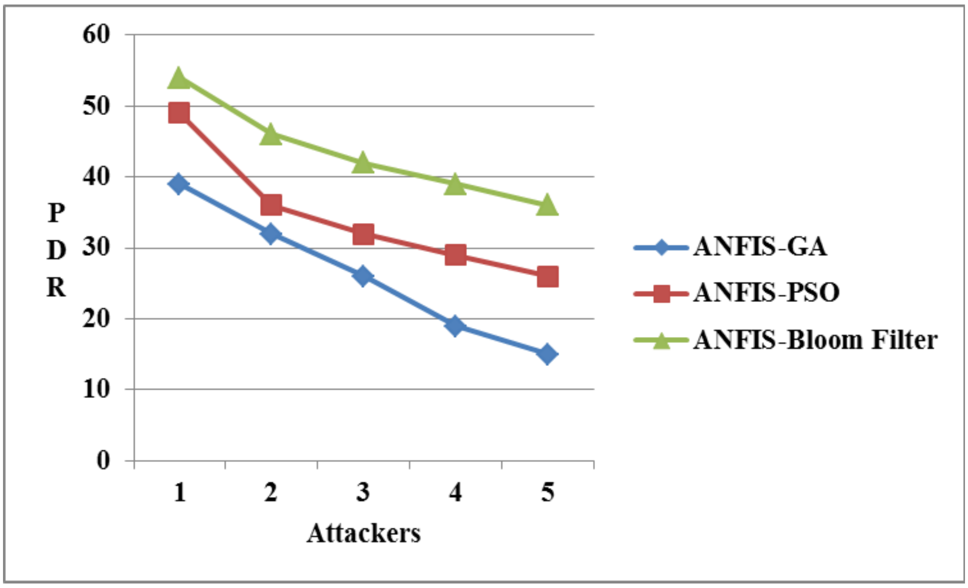


Fig. 4. Validation of Proposed Model with respect to attackers versus packet delivery ratio

ANFIS-GA achieved 39% of PDR, ANFIS-PSO achieved 50% of PDR and proposed method achieved 55% of PDR, when the attacker is 1. However, these techniques achieved 28%, 33% and 42% of PDR when the attacker reaches 3. Finally, when the attacker is 5, GA achieved only 15% of PDR, PSO achieved 28% of PDR and proposed model achieved 38% of PDR. This shows that when the attacker increases, the performance in terms of PDR for each technique's is decreased. Figure 5 shows the graphical representation of proposed model in terms of packet drop rate.

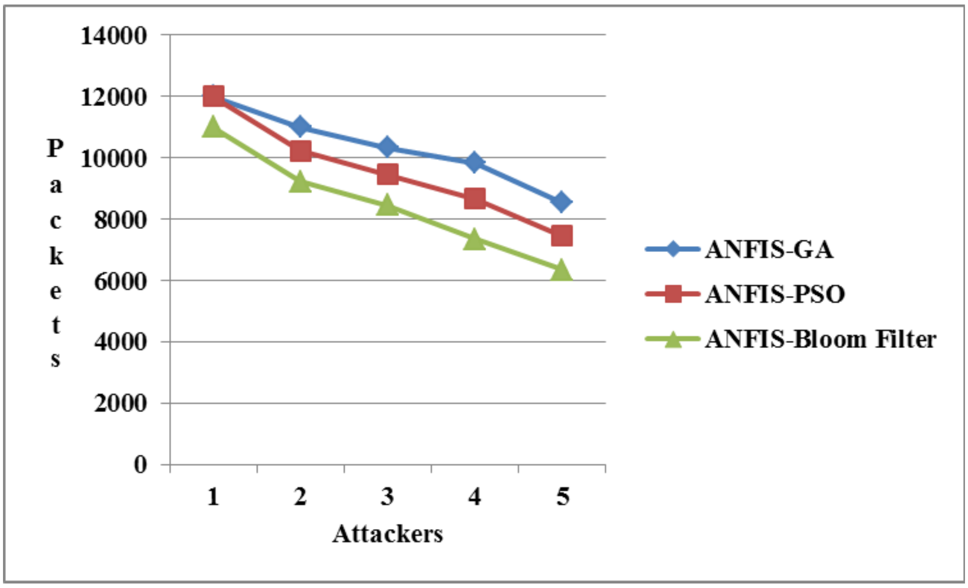


Fig. 5. Validation of Proposed Model with respect to attackers versus packet drop

ANFIS-GA achieved 11800 of packet drop, ANFIS-PSO achieved 10500 of packet drop and proposed method achieved 9000 of packet drop, when the attacker is 2. However, these techniques achieved 9850, 9000 and 7700 of packet drop, when the attacker reaches 4. Finally, when the attacker is 5, proposed model achieved 6100 of packet drop. This shows that proposed ANFIS-bloom filter achieved better performance than existing GA and PSO. Figure 6 shows the graphical representation of proposed model in terms of energy consumption.

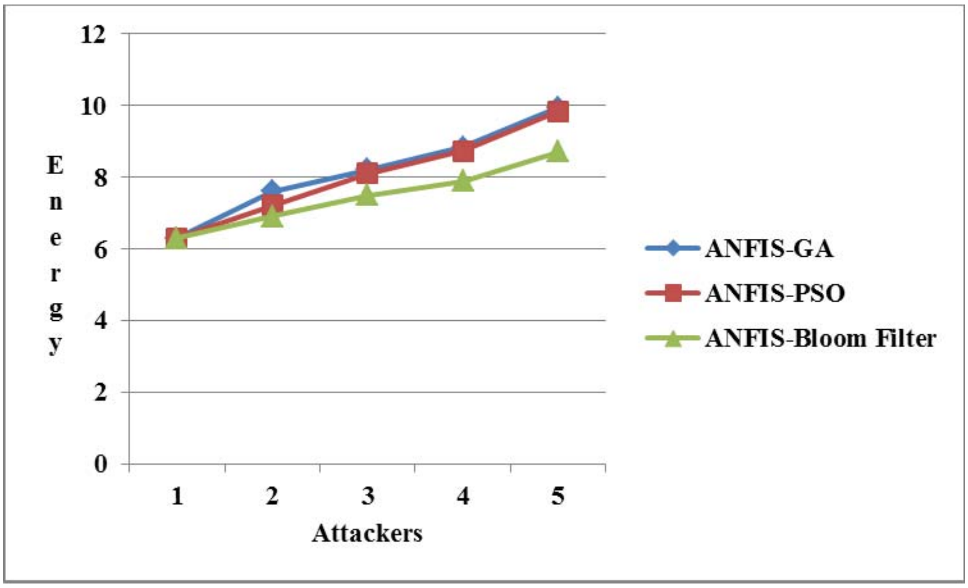


Fig.6 Validation of Proposed Model with respect to Attackers versus energy consumption

Initially, the energy consumption is stable for all the three techniques i.e. 6.1J, when the attacker is 1. The existing techniques such as GA and PSO are stable in energy consumption, when the attacker reaches 3. But, the proposed model provides less energy consumption, i.e. 7.7J for attacker 3, 8.0J for attacker 4 and 8.40J for attacker 5. The above figure proves that the proposed model achieved low consumption of energy and achieved better performance than GA and PSO. Figure 7 shows the graphical representation of proposed model by means of overhead.

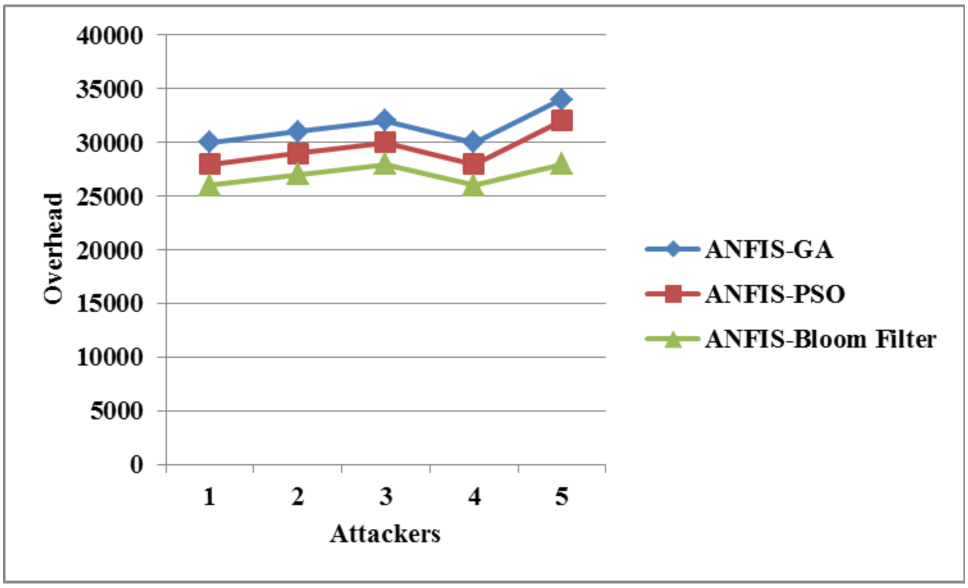


Fig. 7. Validation of Proposed Model with respect to Attackers versus overhead

ANFIS-GA achieved 30000 of overhead, ANFIS-PSO achieved 29200 of overhead and proposed method achieved 26100 of routing overhead, when the attacker is 1. However, these existing techniques achieved nearly 30000 to 33000 of routing overhead, where the proposed model achieved 28750 of routing overhead, when the attacker reaches 3. Finally, when the attacker is 5, proposed model achieved 29010 of routing overhead, where the existing models achieved nearly 34500 to 35000 of routing overhead. This shows that proposed ANFIS-bloom filter achieved better performance than existing GA and PSO in terms of routing overhead. Figure 8 shows the graphical representation of proposed model in terms of node versus delay.

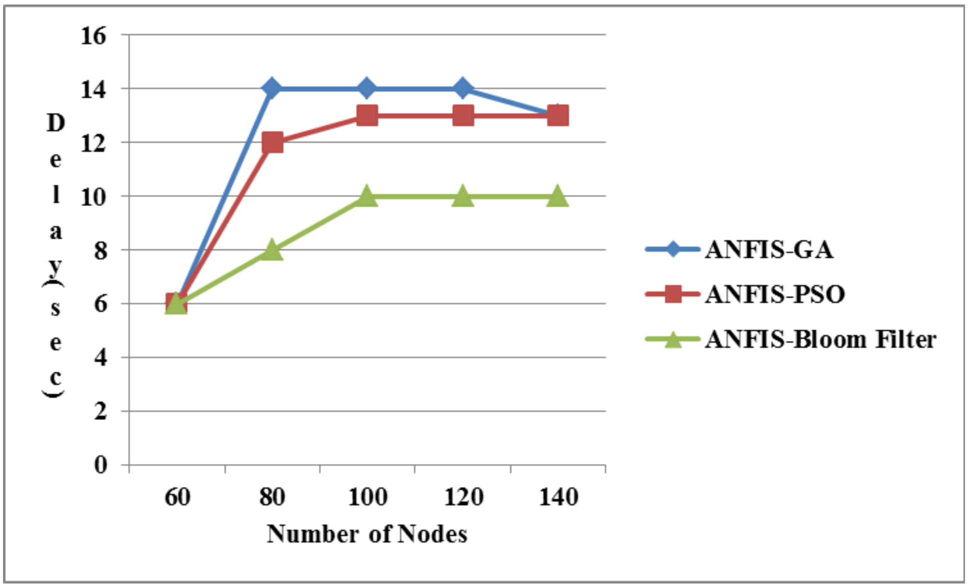


Fig. 8. Validation of Proposed Model with respect to nodes versus delay

ANFIS-GA, PSO and proposed model achieved 6sec of delay, when the number of nodes is 60. However, these existing techniques achieved nearly 12 to 14sec of delay, where the proposed model achieved 8sec of delay, when the node reaches 80. The delay of proposed model is stable (i.e. 10sec) after it reaches the node 100, 120 and 140. But, the GA achieved 14sec and PSO achieved 13sec, when the node reaches 100 and 120. This shows that proposed ANFIS-bloom filter achieved better performance than existing GA and PSO in terms of delay.

5. Conclusion

If an attacker uses multiple identities simultaneously in a Sybil attack, the network is vulnerable. This attack has the potential to cause a great deal of confusion in the network, such as decreasing trust in genuine nodes by leveraging their identities, disrupting packet routing, and so on. As a result, nodes in the network will be able to communicate properly. An assault using Sybil is extremely harmful to mobile ad-hoc networks. An ANFIS with a Bloom Filter in MANET is proposed in this study to identify Sybil attacks. This method relies on the monitoring nodes to communicate from the source to the destination node, exchanging information such as distance, angle, and RSS Variance with the nodes in the two-hop neighborhood. The suspected node is detected using ANFIS logic decisions based on the collected data. The results of this experiment show that the proposed method reduces the overhead of simultaneously hearing all nodes. The cost of listening to every node will be cut in half. As a future work, the performance of proposed method is enhanced by using optimization techniques for optimal path detection.

References

[1] Djenouri, D., Khelladi, L., & Badache, N. (2005). A survey of security issues in mobile ad hoc and sensor networks. IEEE Communications Surveys and Tutorials, 7(4), 2–28.

[2] Hoebeke, J., Moerman, I., Dhoedt, B., & Demeester, P. (2004). An overview of mobile ad hoc networks: Applications and challenges. Journal of Communications and Network, 3(3), 60–66.

[3] A. F. Subahi, Y. Alotaibi, O. Ibrahim Khalaf, and F. Ajesh, ''Packet drop battling mechanism for energy aware detection in wireless networks,'' Comput., Mater. Continua, vol. 66, no. 2, pp. 2077–2086, 2021.

[4] N. Veeraiah and B. Tirumala Krishna, ''Trust-aware fuzzy clus-fuzzy NB: Intrusion detection scheme based on fuzzy clustering and Bayesian rule,'' Wireless Netw., vol. 25, pp. 4021–4035, Jan. 2019.

[5] O. I. Khalaf, G. M. Abdulsahib, and B. M. Sabbar, ''Optimization of wireless sensor network coverage using the bee algorithm,'' J. Inf. Sci. Eng., vol. 36, no. 2, pp. 377–386, 2020.

[6] N. Veeraiah and B. T. Krishna, ''A fuzzy clustering with optimized cluster head selection method in MANET,'' Int. J. Recent Technol. Eng., vol. 8, no. 2, pp. 4972–4976, Jul. 2019.

[7] Garg, R., & Sharma, H. (2014). Proposed lightweight Sybil attack detection technique in MANET. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 3(5), 7142–7147.

[8] N. Veeraiah, ''A comparative analysis of energy efficient multipath routing in MANET,'' J. Adv. Res. Dyn. Control Syst., vol. 12, no. 3, pp. 261–267, Mar. 2020.

[9] Chlamtac, I., Conti, M., & Liu, J. J. N. (2003). Mobile ad hoc networking: Imperatives and challenges. Ad Hoc Networks, 1(1), 13–64.

[10] Douceur, J. R. (2002). The Sybil attack. In P. Druschel, F. Kaashoek, A. Rowstron (Eds.), International workshop on peer-to-peer systems (pp. 251–260). Springer.

[11] Joshi, N., & Challa, M (2014). Secure authentication protocol to detect Sybil attacks in MANETs. International Journal of Computer Science & Engineering Technology (IJCSET), 5, 2229–3345.

[12] N. Veeraiah and B. T. Krishna, ''An approach for optimal-secure multi-path routing and intrusion detection in MANET,'' in Evolutionary Intelligence. Berlin, Germany: Springer, Mar. 2020, pp. 1–15.

[13] R. Prasad and P. S. Shankar, ''Efficient performance analysis of energy aware on demand routing protocol in mobile ad-hoc network,'' Eng. Rep., vol. 2, no. 3, 2020, Art. no. e12116.

[14] S. V. Kumar and V. AnurathaEnergy, ''Efficient routing for MANET using optimized hierarchical routing algorithm (Ee-Ohra),'' Int. J. Sci. Technol. Res., vol. 9, no. 2, pp. 2157–2162, Feb. 2020.

[15] G. M. Borkar and A. R. Mahajan, ''A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks,'' Wireless Netw., vol. 23, no. 8, pp. 2455–2472, Nov. 2017.

[16] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq, and T. Saba, ''Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function,'' IEEE Access, vol. 5, pp. 10369–10381, 2017.

[17] K. T. U. K. Nannapanenia, U. Srilakshmi, and A. Sravyaa, ''Cluster-based collection point energy efficient routing protocol for the mobile sink in wireless sensor network,'' Int. J. Grid Distrib. Comput., vol. 13, no. 2, pp. 787–796, 2020.

[18] M. Anantapur and V. C. Patil, ''Position update secure routing protocol for MANET,'' Int. J. Intell. Eng. Syst., vol. 14, no. 1, pp. 93–102, 2021.

[19] M. Rajashanthi and K. Valarmathi, ''A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs,'' Wireless Pers. Commun., vol. 112, no. 1, pp. 75–90, May 2020.

[20] Karaboga, D. and Kaya, E., 2019. Adaptive network based fuzzy inference system (ANFIS) training approaches: a comprehensive survey. *Artificial Intelligence Review*, *52*(4), pp.2263-2293.

Authors Profile

Dr. K. Sreerama murthy Graduated in B.Tech [CSIT] from JNTU Hyderabad. He received Masters Degree in M.Tech Software Engineering, JNTUH Hyderabad. He received Ph.D. degree in Computer Science and System engineering from Andhra University Visakhapatnam. At Present, he is working as Associate Professor in IT Department, Sreenidhi Institute of Science and Technology, Yamanmpet, Hyderabad, Telangana State, India. His research interests include Data Mining, IDS, Big-Data Analytics, Cloud Computing and Security. He has more than 15 years of teaching experience and he has published patents and several research papers till now in various National, International journals and Conferences, Proceedings.

Dr. Pinagadi. Venkateswara Rao obtained his Ph.D in Computer Science Engineering from Sathyabama University, Chennai, Tamilnadu, India in 2020. He had 14 years of experience in both industry and teaching profession. At present he is working as Associate Professor in ACE Engineering College (ACEEC) in the Department of Computer Science and Engineering. He has published various journals include Indian, International Journal and Conferences. His areas of interest are Machine Learning, Image Processing, Data Structures, and Compiler Design.

Dr. V. Gokula Krishnan is currently working as Associate Professor in the Department of Computer Science and Information Technology in CVR College of Engineering, Ibrahimpatnam, Telangana. He has completed his Under-Graduation (BE) in Anna University, Post-Graduation (M.Tech) in Dr.MGR University and PhD in Sathyabama Institute of Science and Technology, Chennai. He has more than 15 years of experience in the teaching field and also he has published various papers in national/international conferences and journals. His area of interest includes Computer Networks, Computer Architecture, Data Structures, Software Engineering etc.

V. Divya is currently working as Assistant Professor in the Department of Electrical and Electronics Engineering in CVR College of Engineering, Ibrahimpatnam, Telangana. She has completed her Under-Graduation (B.E), Post-Graduation (M.E) in Anna University and she is perusing her PhD in Sathyabama Institute of Science and Technology, Chennai. She has more than 7 years of experience in the industry and teaching field, and she has published many papers in national/international conferences and journals. Her area of interest includes Signal Conditioning System, Nano Sensors, Microprocessors etc.

K. Sathyamoorthy is currently working as Assistant Professor in the Department of Computer Science and Engineering in Panimalar Institute of Technology, Chennai, Tamil Nadu. He has obtained his Under-Graduation (B.E) from Anna University, Post-Graduation (M.Tech) from Sathyabama University and he is perusing his PhD in Vel Tech University, Chennai. He has more than 12 years of experience in the industry and teaching field, and he has published many papers in national/international conferences and journals. Her area of interest includes Data Structures, Computer Networks and Image Processing etc.