Enhancing the Congitive Sensor Network Lifetime and Detecting Blackhole Attack

K.Poonikodi, M.Akshaya, M.Kasthuri, C.Sarathapriya, B.Soundarya
Assiocate Professor, Students
Paavai College of Engineering,Namakkal

Abstract-The biggest issue with cellular networks is the black hole assault. Therefore, it is impossible for the Black hole invaders to quickly take out the complete network. However, in the MANET (Mobile Ad-hoc Network) network, the transaction or contact can be quickly recognized and secured. A unique class of cellular networks are called mobile ad hoc networks (MANET). MANETs are distinguished by their absence of connectivity, which prevents them from having immediate end-to-end pathways. Relay nodes should be used to create links between nodes. Multiple relay nodes can forward a message in the "multi-hop forwarding" manner, which is preferred by MANET routing algorithms, in the hopes that one of the used relay nodes will be able to send the message to the destination node. The quickest-growing network is the mobile ad hoc network (MANET). There is a long inventory of movable nodes on it. The two primary features of MANET are their dynamic structure and absence of centralization. These features make MANETs vulnerable to numerous assaults. The black hole assault is one of the methods used to target the network layer. In a black-hole assault, malevolent servers obstruct data transfer by transmitting false routing information. Black-hole assaults can be either solitary or cooperative in nature. In a singular black-hole assault, the node with the greatest sequence number can only be one malicious node. By going in the correct way, the node source would move in the same direction as the malicious node. The joint black-hole assault uses multiple malicious nodes. One in this assault, a node gets a packet and transmits it to another malicious node. The detection and avoidance of black-hole assaults are very challenging. Systems for detecting and preventing black-hole attacks have been developed by numerous experts. In this article, we identify a flaw in the validity bit-based current approach. This essay also offers a comparison of various academics. Black hole attacks are detected and prevented by the parent node using a binary partition clustering-based method. We demonstrated that our solution beats the existing one by comparing the performance of the suggested solution with that of the existing solution.

Keywords: Mobile Ad hoc Network (MANET), Search for Right Path (SFRP), AODV and AOMDV

I.INTRODUCTION

MANET, also known as a wireless ad hoc network or an ad hoc wireless network, is an acronym for mobile ad hoc network. They are made up of a collection of mobile components that are wirelessly linked in an autonomous, self-repairing network without a permanent infrastructure. Due to the frequent shifts in network topology, MANET nodes are allowed to travel anywhere they please. As they forward data to other designated nodes in the network, each node acts as a gateway. Ad hoc networks are defined as networks with independent end points that want to communicate with one another through pair-to-pair communication. Local area networks are a general term for many ad hoc networks. Therefore, that network there is no requirement for a centralised entry point. Computers and other digital devices can transmit data immediately to one another because of this. Due to the fact that they have only observed and used a limited amount, common users are unaware of the idea of an Ad hoc network.

A malicious node employs its routing protocol in a black hole attack to advertise that it has the quickest path to the target node. This aggressive node advertises the presence of new paths without first consulting its routing database. In this approach, the perpetrator node always has access to respond to the route request, so it can modify and discard the data packet. (Biswas & Ali, 2007). The rogue node respond in a protocol based on flooding will be received by before any real node responds to the asking node, a faked path is established, which is malicious. When this path was configured, the node now decides whether to discard packets or forward them to an unidentified location.

1.1 PROBLEM STATEMENT

Prior research on MANETs primarily addressed various security risks and assaults, including DoS, DDoS, and impersonation, as well as wormhole, jellyfish, and black hole attacks. One of these assaults, the Black Hole attack, which affects MANET, is assessed using a reactive routing protocol called Ad-Hoc on Demand Distance Vector (AODV), and the impacts of this attack are explained by highlighting how MANET performance is disrupted. It has received very little notice that studying the using both reactive and proactive protocols, the Black Hole attack's effect on MANET is examined, along with the attack-resistance weaknesses of each protocol. Both these categories of attacked protocols and the effects of the assaults on MANETs require attention. In this paper, reactive and preemptive methods called AODV and OLSR are used to analyze Black Hole attacks in MANETs.

II.LITERATURE SURVEY

2.1. PRANJALI VARSHNEY-By creating and changing routing tables whenever mobility happens, MANET and some DTN routing methods offer forwarding. Given that topology structure is extremely dynamic and movement is frequently unexpected, we think this method is inappropriate for a PSN. Instead of exchanging a lot of control data to build unstable routing structures that might only be able to detect network "noise," we would prefer to look for network properties that are less prone to volatility than mobility. By creating and changing routing tables whenever mobility happens, many MANET and some DTN routing methods offer forwarding. Given that topology structure is extremely dynamic and movement is frequently unexpected, we think this method is inappropriate for a PSN. Instead of exchanging a lot of control communication to produce faulty routing structures, which may only catch the network's "noise," so we prefer to look for network properties that are less erratic than movement. PSNs are created by individuals. Social measures are therefore inherent characteristics to direct data forwarding in these types of human networks. Furthermore, we can use these algorithms in real-world settings if we can locate these social mobility patterns online in a decent realized manner.

2.2. PRATYAKSHGOE-Sharing information and data over an unprotected route makes it vulnerable to theft and assault, making encryption one of the most important technologies for data authentication. This article proposes a novel method of digital signature scheme that combines Ong, Scour, and Shamir signature scheme with elliptic curve cryptosystem (ECC). (OSS). In addition to OSS signature equations, a self-invertible 44 key matrix will be used, increasing total security and effectiveness against cryptanalytic assault. Its strength is proclaimed and authorised based on extensive execution and security analysis findings. If existing systems are compromised, the suggested method can be used as a secure alternate protocol.

2.3.PRAKHAR GUPTA, Ad hoc networks are vulnerable to assaults because they are created according to specifications without the assistance of a supervisor and each node serves as a router. This article suggests an AODV algorithm with reliability-based protection against malicious nodes. It takes into account the so-called "black hole attack," in which a malicious node infiltrates the network by transmitting a false RREP with a high sequence number and drops all the messages rather than passing them. The suggested approach successfully boosts speed and packet delivery ratio while decreasing end-to-end network latency. A study of the Sybil assault, a dangerous strike on sensor networks. In the Sybil assault, an evil node acts in a if there were more nodes, for instance by pretending to be other nodes or assuming fake names. In the worst scenario, an attacker could use a single physical object to create an infinite number of extra node IDs. If a local entity is unaware of distant entities physically, it only perceives them as informational abstractions that we refer to as identities. Otherwise, when the local entity chooses a subset of identities to redundantly conduct a remote action, it could be tricked into choosing a single remote entity multiple times, defeating the redundancy. The system must guarantee that distinct identities pertain to distinct entities. The creation of numerous identities is referred to as a Sybil assault on the system. It is alluring to picture a Similar to the PGP web of trust for human entities, this system uses established identities to advocate for other identities so that an entity can accept new identities by believing the aggregate guarantee of many (presumably independent) signatures. However, our findings demonstrate that a Sybil assault can seriously damage the original generation of identities, undermining the chain of vouchers, in the lack of a trustworthy identity authority (or unrealistic beliefs about the resources accessible to an attacker.

III. EXISTING SYSTEM

Since putting transmitters in numerous places is much more difficult than obtaining extra computation or memory resources, Black hole defense methods used in the current system rely on resource testing of wireless channels. Black hole attackers are difficult to spot and get rid of from the network. The use of intermediate nodes in transactions from the parent node to the target node lowers the issue with time delays. However, the intermediary node acts as a black hole offender node, which causes the transaction's problems and damages or modifies the data. The message or changed message cannot be received by the target node. The Black Hole attacker node should be identified by the trustworthy Authority or group manager, but it cannot be removed from the network. Black with signal prints Any user in an open wireless network can find out which of its one-hop neighbors aren't Black hole nodes thanks to hole discovery techniques that don't require any a priori confidence in observers. Prior to recording what is seen, participants alternately disseminate probe packets to the other participants. Then, these findings are discussed. Following this conversation, each person shared their views along with those of the other four. Finally, for the signal print-based Black hole, each person chooses a unique subset of witnesses that they believe to be truthful. As a result, the Black hole component can be removed from the network, securing all group communications. to employ the RSA formula along with a private key and hashing methods. Here, the optimal route is chosen based on the results of transmitting Search for Right Path (SFRP) packets to the target by various paths the less-hop count measure. The Path Approval (PA) is then prepared, and the nodes add the PA packet using the secret key they obtained from the PKI. (Public-Key Infrastructure). The node then used the digest algorithm to calculate this message. The original PA packet is then appended by the node with this calculated digested data. After that, the paths approve source node unicast.

3.1 DISADVANTAGES

- Occur the traffic problem.
- Transaction can’t to be secured and attacker easily modify the data.
- Can’t identify the attacker is present of not in the hop nodes.

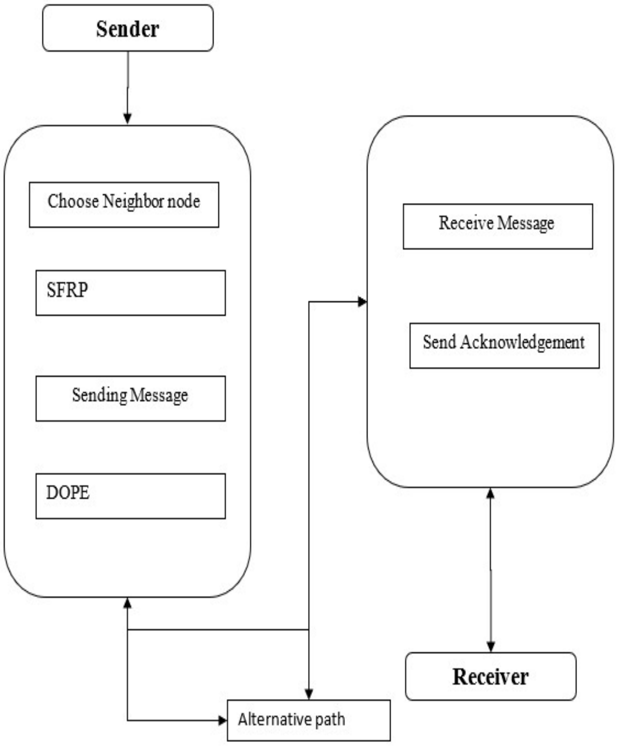
VI. PROPOSED SYSTEM

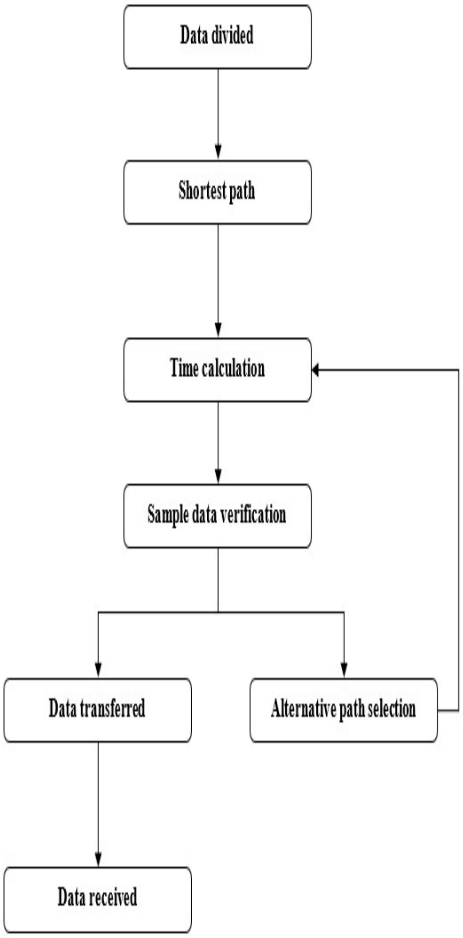
The two processes that make up the proposed system have been used to transmit data securely using the AODV and AOMDV protocols, and the results have been compared. Both AODV and AOMDV first use the Search for Right Path (SFRP) intent, which includes two different types of data/information, to find the location. The first one, a control file, is referred to as changeable data or information. This data can be read out by intermediate hubs and the final target. A data packet is a source of mutable information or data that is connected to the source. Although the control packet cannot be digitally verified, changeable information such as data packets can. To find the destination node, the source first sends an SFRP to each of its neighbors. the center Nodes that have been placed now have the same SFRP data with a fresh, revised journey count. Furthermore, SFRP will continue forwarding if the nodes do not meet the destination's step count. If the target IDs agree, the destination ID can be found by the SFRP packet. The target node then divides the data payload and the control packet into their respective parts. The information in the control packet is used to locate the target and is connected to the intermediary router and the destination. It Elliptical curve digital signature algorithm (ECDSA) usage Data transfer is used.

4.1 ADVANTAGES

- Securely transfer the data from source to the destination.
- The attacker can’t to be modify the original data.
- Reduce the network traffic problem.

4.2 SYSTEM ARCHITECTURE





4.3 FLOW DIAGRAM

V. SYSTEM IMPLEMENTATION

5.1 MODULES

- Network formation.
- Path Selection
- Identify the Black hole attacker.
- Performance evaluation.

5.2. MODULES DESCRIPTION

5.2.1 Network formation

A link has been formed between many components in a wireless network. Mobile, notebook, PC, and other components are among them. The nodes must therefore be in communication with one another. The MANET protocol must be used for the transaction, and the transmission must be extremely safe. The network link is primarily utilized for file sharing and information interchange between nodes as well as communication with each other's nodes. Because the network is wireless, network transactions are dependent on the intermediary component. The component is thus known as a hop node. The transaction from the source node to the target node via an intermediary node is under the authority of the MANET protocol. Based on the access point, the network service area is determined. Capability for bandwidth. The routing algorithm links each node to a different hop node.

5.2.2 AOMDV

Use the Routing protocols to determine the shortest route between the source and target nodes prior to the transaction. The distance and number of intermediary nodes determine the shortest route. Next, determine the path that is the shortest between the source and target nodes. The Dijkstra method originally indicates on the map that the distance to every other intersection is infinite. This is done to indicate that those junctions have not yet been reached, not to suggest that there is an endless distance. Some variations of this technique merely leave the lengths between the junctions unlabeled. Select the present intersection after each repetition. The present intersection will serve as the beginning position for the initial iteration, and the distance from it will be zero. For further The present intersection will be the most nearby unexplored intersection to the beginning spot after all iterations. When a source and a destination need to interact, the AOMDV routing algorithm is used to find a path for MANETs. During the single route finding procedure, the multi-path routing protocol finds numerous paths. When the main route breaks, these additional paths can be used as backup routes or to distribute the burden. AOMDV, like AODV, employs a hop-by-hop routing strategy and is built on the distance vector concept. Additionally, AOMDV uses a route finding process to identify routes on demand. AOMDV discovers numerous routes in a single route finding process, in contrast to AODV. All identical RREQs are deleted in AODV, but AOMDV searches for opportunities to obtain an alternate path with each RREQ copy. In AOMDV, numerous reverse routes are established at both the target and intermediate nodes during RREQ propagation from the source to the latter. To create multiple forward routes to the target at the source and intermediary nodes, multiple RREPs travel these reverse paths back. The main goal of the AOMDV protocol is to identify such paths quickly using a flood-based route discovery technique while also assuring that the multiple paths are loop-free and distinct. The local application of AOMDV route update rules at each node is essential for preserving loop-freeness and disconnected characteristics.

5.2.3 Identify the Black hole attacker

When the Black hole intruder is present in the transaction's hop node, data from the original node is lost and given to the attacker. As a result, the issue is solved using this method's example data proof. The Mobile Ad hoc Network (MANET) Black Hole assault describes an assault that is caused by malicious nodes that draw data packets by misrepresenting themselves as a new path to the target. Black hole attacks refer to attacks where the attacking node responds to the Search for Right Path (SFRP) with a false Path Approval (PA) and then presents itself as the routing node with the most recent path by producing a bigger sequence number. In this assault, the competing node draws packets, but instead of sending any of them to their intended location, it ditches the mall. The packets sent by the nodes do not arrive at their intended location as a result of this assault. When an attacker node stops a channel, AOMDV typically selects a different route. The issue mostly arises when several attacker nodes obstruct all other paths and the attacker nodes are functioning as routers that pretend to be legitimate ones. Following that, begin the procedure along the shortest route and examine the example data exchange. Send the original data to the target node if the black hole attacker is unable to show the intermediate node.

5.2.3.1Algorithm

Step1:The source transmits Packet Request P to each neighboring node

Step 2: This node receives the message and gets ready to make a packet request if it is the intended node. All nodes will forward the Search for Right Path (SFRP) message to the next node in order to find the destination if it is not. In the event that the target cannot be located, a Detection of Path Error (DOPE) notification will be sent.

Step 3: The routing database will be used to store every potential route, and an appropriate route will be chosen for Path Approval. (PA).

Step 4: Once the data packet and control packet have been separated from the SFRP, the destination will apply the ECDSA signature hash function to the data packet to generate a hash value and send it to the source.

Step 5: Each intermediary node will verify the hash value sent by the neighbor node and approve the packet and forward to the following node if the hash values match. If not, it will discard the file and pick an alternative route.

Step 6: Step 5 will be carried out up to the source. It will compare the signature with the first component when it gets to the source. All subsequent ID will not be confirmed and will be deleted if it fails.

Step 7: Currently, Daffier-Hellman key exchange is used to match the keys after the PA has gotten them. The source will begin transferring data to the recipient if the key fits the route, otherwise it will be discarded. To AOMDV If a key fits, data will be transferred to multiple paths using the same technique, which multiple paths will use.

5.2.4 Performance evaluation

Therefore, the technique must be one of transaction-time data security. Without a trustworthy authority or group administrator, the source can be examined to determine whether a Black Hole attacker is present on the intermediary in the transaction. The cluster node side of the transaction is where the security is verified; it cannot be relied on any other cluster head node. Therefore, the technique should evolve to account for changes in security, transaction volume, packet loss issues, and transaction throughput.

VI.CONCLUSION

A process for detecting and avoiding black hole attack in MANET. Here, mainly the security deals with confidentiality and authentication of data packets. After separating the information into mutable and non-mutable, two different algorithms are considered for evaluation. The non-mutable information approaches with unique hash value using the ECDSA algorithm. Then the data transfer starts after sharing the keys of both source and destination. This protocol assumes that, each node has a pre-distributed secret key. This procedure provides a safe path discovery to transmit data for both AODV and AOMDV routing protocols. The results achieved from the method indicates better performances than a normal simulation result of these protocols. The Path Approval (PA) packet is delivered by a secure hash algorithm. Then the data transfer starts by exchanging secret keys of both source & destination. This two processes ensure that if any malicious node attacks, the hash value will change. The changed value will not match with the next node so that the whole path will be discarded and Path Approval (PA) will be sent in a secure path where the hash value will remain same until reaching the source. Then when the Path Approval (PA) reached the source, the source node exchanged the secret key value with the destination to match the value and check if the path is actually safe to transmit data. By this technique, all insecure paths have been avoided and the safest path has been chosen for data transmission. For this, all the performance results give better output than normal. In future, it is expected to apply this technique in other protocols and merging of a cryptography algorithm with Daffier-Hellman key exchange to make a better and secure method than the proposed method. In future, the already proposed method or some kind of modified method can be also used to remove the malicious nodes by repairing them (malicious nodes) to get further better performance and implementation of more performance matrixes for both AODV and AOMDV routing protocols.

REFERENCES

[1] Shelbala Solanki & Anand Gadwall, "Hybrid security using Digital Signature& RSA", vol. 6 (3), 2015.

[2] Nagarajan and M.Madheswaran - ‘Experimental Study and steady state stability analysis of CLL-T Series

[3] Parallel Resonant Converter with Fuzzy controller using State Space Analysis’- Iranian Journal ofElectrical &amp; Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[4] Mrs Preeti. A. Aware, Mrs AmarjaAdgaonkarn& Mr SaurabhSuman, "Black hole attack prevention on AODV in," IJSTE -International Journal of Science Technology & Engineering, vol. 4, no.1, Year 2017.

[5] Romana Rahman Ema, Ashraf Akram, Md Alam Hossain &SubrataKumar Das, "Performance analysis of DSDV, AODV AND AOMDVrouting," Global Journal of Computer Science and Technology: Network, Web & Security, vol. 14, no. 6 Version 1.0, Year 2014.

[6] AbdulssalamA.Alafi, Aditi Agrawal, A.K Jaiswal & Rajeev Paulus, “Preventing Black hole attack from Routing Path in MANETs by Secret key and hashing," International Journal of Emerging Technologies in Engineering Research (IJETER), vol. 5, no. 4, Issue 4,April(2017).

[7] Singh, Primed Kumar, and Govan Sharma., "An efficient preventionof black hole problem in AODV routing protocol in MANET" , pp.902-906, 2012.

[8] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. “Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter” Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[9] AfdhalAfdhal, Sayed Muchallil, HubbulWalidainy, QodriYuhardian., “Black hole attacks analysis for AODV and AOMDVrouting performance in VANETs" , Year 2017.

[10] Parth Sehgal, Nikita Agarwal, Sreejita Dutta, P.M.Durai Raj Vincent, “Modification of Daffier-Hellman algorithm to provide more secure Key exchange”, “International Journal of Engineering and Technology(IJET)”, vol. 5, No 3, Jun-Jul 2013.

[11] Nitin R. Chandrana,Ebin M. Manuel*,”Performance analysis of modified SHA-3”, Year 2015.

[12] Uday Singh Kushwaha, P. K. Gupta, S. P. Ghrera, ”Performance evaluation of AOMDV routing algorithm with local repair for wireless mesh networks”, 3 June 2015.

[13] C.Nagarajan and M.Madheswaran - ‘Stability Analysis of Series Parallel Resonant Converter with Fuzzy

[14] Logic Controller Using State Space Techniques’- Taylor &amp; Francis, Electric Power Components andSystems, Vol.39 (8), pp.780-793, May 2011.

[15] M.Kannan, R.Srinivasan and G.Neelakrishnan, “A Cascaded Multilevel H-Bridge Inverter for Electric Vehicles with Low Harmonic Distortion”, International Journal of Advanced Engineering Research and Science, November 2014; 1(6): 48-52.

[16] Nita Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri,”Improving AODV protocol against Blackhole attacks”, Vol 2, March17-19, 2010.

[17] C.Nagarajan and M.Madheswaran - ‘Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID

[18] Using State Space Analysis’- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[19] R.Baskar, R.Jayaprakash, M.Balaji, M.Kannan, A.Divya and G.Neelakrishnan, “Design of Nanoscale 3-T DRAM using FinFET”, IOSR Journal of Electrical and Electronics Engineering, November-December 2013; 8(1):1-5.

[20] Dr.C.Nagarajan, G. Neelakrishnan, V.Sundarajan, and D.Vinoth, “Simplified Reactive Power Control for Single-Phase Grid-Connected Photovoltaic Inverters” International Journal of Innovative Research in Science, Engineering and Technology, May 2015; 4(6): 2098-2104

[21] C.Nagarajan and M.Madheswaran - ‘Experimental verification and stability state space analysis of CLL-T

[22] Series Parallel Resonant Converter’ - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372,Dec.2012.

[23] Dr.C.Nagarajan, G. Neelakrishnan, V.Sundarajan, and D.Vinoth, “Simplified Reactive Power Control for Single-Phase Grid-Connected Photovoltaic Inverters” International Journal of Innovative Research in Science, Engineering and Technology, May 2015; 4(6): 2098-2104

[24] M.Kannan, R.Srinivasan and G.Neelakrishnan, “A Cascaded Multilevel H-Bridge Inverter for Electric Vehicles with Low Harmonic Distortion”, International Journal of Advanced Engineering Research and Science, November 2014; 1(6): 48-52.

[25] G.Neelakrishnan, M.Kannan, S.Selvaraju, K.Vijayraj, M.Balaji and D.Kalidass, “Transformer Less Boost DC-DC Converter with Photovoltaic Array”, IOSR Journal of Engineering, October 2013; 3(10): 30-36.

[26] R.Baskar, R.Jayaprakash, M.Balaji, M.Kannan, A.Divya and G.Neelakrishnan, “Design of Nanoscale 3-T DRAM using FinFET”, IOSR Journal of Electrical and Electronics Engineering, November-December 2013; 8(1):1-5.