International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-2, Issue-4, July 2015

Good Neighbour Node Detection Technique in Manets Using Enhanced QOS GNDA

Mrs. Pallavi Patil , Mrs. Arpana Morey
Department of Computer Engineering
Pillai's College of Engineering and Technology

ABSTRACT

As MANETS (Mobile Ad hoc Networks) is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. Security in Mobile Ad-Hoc Network is the most important aspect for the basic functionality of network. MOBILE Ad hoc Networks (MANETs) are wireless networks which are characterized by dynamic topologies and have no fixed infrastructure. As such detection of a good neighbor node is a necessity. In the routing protocol called Quality of Service Good Neighborhood Node Detection Algorithms (QOS-GNDA) author find the good node but if malicious node present in network and if it makes entry in routing path then it causes security threat to sensitive data so we find the new Enhanced Quality of service Good Neighbor Node detection technique .we use Enhanced Highly Secure Approach against Attacks on MANETs (EHSAM) to overcome the data tempering problem.

Keywords: MANETs, Adhoc routing, AODV, Signal strength, Flow capacity, Relative position, malicious node.

1 .INTRODUCTION

There are several competent routing protocols available in mobile ad hoc network. Some protocol used table driven approach where some protocol used reactive approach. Selection of appropriate protocol for routing is essential factor for efficient and effective communication of data. While selecting the protocol various aspects need to count such as low network overhead, high throughput and high packet delivery ratio and delay in packet forwarding.

In today's era, security is essential for any system. MANETs should have secure way of communication & data transmission. The system should defend all kind of active & passive attacks, internal & external attacks. Various attacks such as black hole attack, grey hole attack, tunneling attack, flooding attack, selfish node misbehaving, spoofing, eavesdropping, Sybil attack, rushing attack, Denial of Service attack (DoS), impersonation attack, routing table overflow attack cause threat to MANET.A MANET is open to all these attacks due to communication among the nodes is on trust based, no central point for managing the network, limited resources such as battery and bandwidth, continuous change in topology & no authorization for new nodes before joining to network. Various approaches are used to overcome or to avoid network level attacks in different protocols. Mainly various encryption methods such as RSA, MAC, hash code etc. used to provide authentication & integrity of message. Some methods use digital certificates & public key infrastructure to achieve security goals in ad-hoc network. Watchdog & path rater used to avoid packet dropping attack & selection of path with high rating. By use of various methods & techniques to achieve security might increase overhead over the network. Each node has to do additional computations to achieve high security, which may increase overhead on node. The main aim of any approach should be provide effective and secure way of communication with minimum overhead, less computation. Various approaches are attack specific. That makes system vulnerable for colluding attack. To avoid such attacks various approaches needs to be used in combination

This paper is organized as follows. Section 2 describes the impact of malicious neighbor nodes. In section 3, some of the good and malicious neighbor detection methods are reviewed. Section 4 presents proposed methodology for enhanced good neighbor node detection based on EHSAM using QOS-GNDA. Section 5 depicts consultation.

2. IMPACT OF MALICIOUS NODES

The nodes in MANET have limited battery power and bandwidth, and each node needs the help of others to get its packets forwarded. The different protocols in MANETs assume that all the nodes are cooperative and whenever a node receives a request to relay traffic, it always does so truthfully. However the experience has shown that as the time passes there is a tendency in the nodes in an ad hoc network to become selfish. The selfish nodes are not malicious but are reluctant to spend their resources such as CPU time, memory and battery power for others. The problem is especially critical when with the passage of time the nodes have little residual power and want to conserve it for their own purpose. Thus in MANET environment there is a strong motivation for a node to become selfish. The working of Adhoc network is based on packet forwarding using neighbor nodes, the source or the sender node must rely on intermediate nodes. The dynamic nature of network topology in Adhoc network leads the problem for nodes like, limited bandwidth, hidden terminals, transmission errors, and battery constraints, selfish nodes. The nodes affected by this gives poor performance ultimately the network throughput and network protocol affected and the performance of the network is decreases.

3. EXISTEM SYSTEMS

In MANET there is lack of central administration system which monitors the nodes and find out which node is misbehaving. Here each node forwarding the packet to next node on simply trusting it and increase the threat to system. Attacker can easily make any node to compromises on security goals by launching internal or external attack.

Wireless link present between the nodes also makes security concern because attacker can simply overhear the data passing through these links or even participate in the network and modifies the data. Thus, routing is a basic operation for the MANET. Because traditional routing protocols cannot be directly applied in the MANET, a lot of routing protocols for unicast, multicast, and broadcast transmission have been proposed since the advent of the MANET.

Perkins Charles E. and E. M. Royer [1] Proposed an algorithm fro optimizing the routing issues by using AODV [1] while Umang Singh et.al, [2] suggest a GNDA algorithm. This protocol finds good neighbor node using parameters like Transmission range, Power of node, Signal strength, Capacity of node for packet forwarding and Relative position of node. But this protocol fails to reduce the congestion because packet forwarding is considered only for high bandwidth data. In reality, low bandwidth packets also exist which may lead the network towards congestion. Also, as the network size increases, cost also increases. Reddy et.al. [3] Proposed reliable AODV routing protocol which enhances network performance by selecting stable nodes (i.e., only good neighbor nodes) for network formation. All information related to reliable nodes are stored in routing table which improves performance of routing protocol in terms of good communication and stable route. Quorum-Based Neighbor Discovery is proposed by Sina et.al.,[4]. This approach is a deterministic handshake-based algorithm using quorum systems. A quorum is the minimum number of nodes to be present at an assembly. Quorum-based neighbor discovery allocates a quorum system for all elements of universal channel set. During each time interval one or two channels are selected for sending or receiving the advertised message. Transmission is done through available channels, thus skipping the unavailable channels. The size of quorum system used on the whole network is known as the upper band of discovery length. Biradar et.al.,[5] have effectively demonstrated the process of neighbor node selection in MANETs using reliability pair. The reliability pair formation and computation of reliability pair factor for every established reliability pair is triggered by jointly handling the parameters such as remaining battery power of nodes, mobility of nodes, distance between the nodes and differential received signal level of neighboring nodes. The reliability pair is formed such that link stability is maximized while link cost is minimized. For each node, whenever node changes its location, reliability factor is calculated. This will result into increased network overhead. Wang Gang et.al.,[6] uses phoenix network coordinate system which maps each node as incoming vector and dimensional outgoing vector. Network Coordinate (NC) which provides efficient distance prediction with scalable measurements brings benefits to various network applications. Phoenix Network Coordinate system is a recently proposed dot product based NC system with high prediction accuracy and better robustness. This system has considered only distance while ignoring other parameters like signal strength, flow capacity, battery power etc. Saleem Bhatti et.al.,[7] proposed Dynamic Timer Based on Multi-Increase Additive Decrease algorithm(DT_MAID) in which adaptive neighbor detection is done by minimizing the route discovery side effects. Pedro M. et.al.,[8] proposed a Geographic Multicast Routing(GMR) which is a cost based neighbour selection policy at each round trip. But this solution is applicable only for small number of destinations. Pallavi Patil et.al.[11] proposed neighbour node detection technique using QOSGNDA using different parameters like Transmission range, CBC(current bandwidth) etc. This protocol finds good neighbour node but this protocol fails to overcome the problem related security of data.

Obaidat et al. [12] proposed an Enhanced Highly Secure Approach against Attacks on MANETs (EHSAM). This paper enhances the HSAM protocol by introducing a more efficient approach to secure the route selection phase. Their approach addresses the problem of packet dropping and packet tempering attacks in MANET. When routing operation performed between the source node and destination node pair they used mock packets instead of actual data packets to check trustworthiness of selected path for communication. Packets are split into 48 bytes chunks by source node .Their approach uses hash code to check integrity of data by destination node. They used counters cpkt while sending packets and cmiss when packet is missed. They calculated RTT of data frame if it exceeds 20ms value then packet might be dropped and increment the counter cmiss.If RTT equal or less than 20ms then connection is good. If there is mismatch in hash code sent by source node and computed by the destination node then there might be data tempering attack present. Then source node gets notified by destination node. This approach is unable to focus on false routing attack and worm hole attack may present in that path. Only suspicious path is detected but node which is actually discarding packets is unable to detect. Mamatha et al. [13] proposed a highly secured approached against attacks in MANETs (HSAM). This approach is primarily focuses on identifying misbehaving links, packet dropping and packet tempering attacks. HSAM provide approach to overcome on these attack and such malicious nodes should be identified. Such compromised node makes entry in the routing path and disrupts the network. This algorithm uses two main approaches are counter and hash code. The packets are divided in to sub-packets. When packet sent from source the counter at source named as Cpkt incremented. This counter keeps track of how many packets are sent from source node. Hash code is code also sent among these packets. When sub-packets are received at destination node they are reconstructed and compute the hash value. If hash code is matched then no data modification attack happened but if data is tempered then hash code does not get matched then acknowledgement send to source node with field confidentiality lost field set to one. If acknowledgement does not come within time limit then it is assumed those packets are lost and increment the counter Cmiss. This method uses flow of conservation which strongly state that number of packets sent from source node should match with number of packets received. When source node receives acknowledgment with confidentiality lost field also ratio of Cmiss/Cpkt above the limit of tolerance. There is possibility of data modification and packet dropping attack. Source node discards that path.

This method cannot provide solution for the misrouting attack. When the path is discarded then source node again does the path discovery process which increases the overhead on the network**.**

4. PROPOSED MEHODOLOGY

In the proposed system, we are finding good neighbor node as well as secured data transmission at the time of link establishment only. Various parameters like Transmission range, Power of node, Signal strength, Capacity of node for low as well as high bandwidth packets forwarding and Relative position of node are utilized for finding good neighbor node. These parameters help in minimizing end to end delay and packet dropping ratio. It also removes congestion in network and improves performance of the routing protocol and hence performance of the network. In existing approach Pallavi Patil et.al., [11] decide a particular node to be good or bad based on Performance parameters such as Transmission range, Power of node, Signal strength, Capacity of node for required bandwidth packets Forwarding and Relative position of node .Our works aims to prevent mobile ad hoc network from network layer attacks such as black hole attack, greyhole attack and worm hole attack. If malicious node present in network and if it makes entry in routing path then it causes security threat to sensitive data. This approach tries to avoid packet dropping and packet tempering attack. It tries to prevent malicious node to come in the network again. When actual data packets send over network after route discovery process from source node and destination node then any misbehaving node is present in the path then there is risk of sending data over the network. Our approach uses mock data packets before sending actual data packets to check trustworthiness of path selected in route discovery. These mock packets are divided in to 48 bytes data frames which contain source address, destination address, hash value and message to send. If any malicious node present in path and tries to modify the data then there will be change in hash value from that malicious path can be identified .Public key cryptography is used to authenticate a node in the network. A node has valid public and private key pair able to encrypt and decrypt the message. Unauthenticated node cannot take part in packet forwarding process. To forward the packet it have to decrypt the data frame and match with destination field with own address. If address is not matched then packet is forwarded to next hop node. Use of public key cryptography provide guaranty of authenticity of node. Confidentiality of message is maintained. In this proposed work we focus on generalized solution on network level attack. Due to use of mock data packets no affect on actual data communication. Trustworthiness of path is tested before the actual communication starts. During mock packet forwarding process there might be overhead on network but when actual data communication started then there will be less overhead due to no need of using any encryption method or overhearing is needed. This integration of hashing, public key cryptography and timer used to check packet forwarding behavior increases security level of the MANETs. To detect the wormhole attack in which one malicious node create tunnels to other node and forwards packets through that tunnel. To detect such attacks our approach uses timer with each node. When any node forwards data packets then it start timer and waiting for overhearing from next hop. If overhearing come within that timer that means packet is not tunneled or discarded. If packet is discarded or tunneled then overhearing will not come or come after expiration of timer. If node exceed the threshold value of such count then there is tunneling attack or packet discarding attack present. To eliminate such node from coming into next path of communication node black list is maintained at source node. If any malicious node tries to tunnels the packet or discards the packet then such node is notify to source node by sending alarm message as RERR message send in the QOSGNDA protocol. Source node maintain list of such node and in next route discovery that nodes are avoided form coming into path of communication. If there is mismatch in the hash value at destination then data tempering is happened in path so path is suspicious path and path is informed to the source node as RREP message send in QOSGNDA protocol. Source node maintain path black list in which suspicious path added. In next route discovery process such path are avoided. If path is malicious node free then actual data packets are sending between the source and destination. If any misbehavior is detected then route discovery process is started by the source node. Algorithm used to detect malicious node and path.

Algorithm:

- A RREQ is sent by the Source(S)
- Source S receives RREP from the destination(D)
- Route from S to D through regular GNDA protocol
- Each node maintain table

Next hop id	Count

- Mock packets are send before sending actual data packets to check path is malicious or not
- Mock data packets are split into 48 bytes chunk.

Algorithm

STEP 1**:** Initialize Total number of nodes in the network
STEP 2: Initialize TTr of the network
STEP 3: Broadcast Hello message
STEP 3.1: Send MOCK packet

1) Source node S creates mock packets of 48 bytes
2) For each packet to be sent by S:Construct mock data frame with Source node address, Destination node address, message to be sent and hash code
3) When source node sends data frame, it encrypts that frame.
4) Source node or any intermediate node starts timer while forwarding the frame
5) Source node or any intermediate node overhears to next hop whether frame is forwarded or not .If overhearing message does not come within the timer then increase the Count
6) If Count Value exceeds the threshold value then alarm message sent to source node with misbehaving node id. Alarm message sent such way the RERR is sent to Source node**.**

STEP 4: Receive Hello message
STEP 4.1: Receive MOCK packet

1)Source node maintain node black list of such misbehaving node so when next route discovery phase starts then source node remove path which having these nodes.

2) Intermediate node decrypts the frame and checks whether destination address is matched with its address if not then it forwards frame to next hop.

3)If destination address field matched with node address then packets are reconstructed at destination and hash value is

computed if it is matched then path is ok but if it is not matched then path is not malicious node free then destination node sends acknowledgement to Source node acknowledgement to Source node.

STEP 5: Calculate time, of reaching Hello message

STEP 6: Compare NTr and TTr

STEP 6.1: if NTr > TTr then Decrease the NTr and go to step: 6

STEP 6.2: else go to step 7

STEP 7: Calculate signal strength

STEP 7.1: I f signal strength > = Threshold then go to step: 8

STEP 7.2: else it is a weak signal so go to step: 4

STEP 8: Calculate flow capacity

STEP 8.1: If flow capacity is equal to CBC then store node address (Good node)

STEP 8.2: else Bad node

Source node maintain path black list.

STEP 9: Send RREQ through good node

STEP 10: Source node starts route discovery process

If any path matches that path black list and includes nodes from node blacklist then source node discards the route.

STEP 11: If path is ok then source node starts sending packets to destination node.

5 .SUMMARY

This protocol improves the performance of QOSGNDA in terms of security of data in network. This approach can be applicable for real time scenario. Although the promising results are shown, still there is much room for improvement. Limitation of this approach and proposes possible extensions of the research to improve the performance of this system and have this system more applicable to general application. For finding good node with data security we are applying the proposed Enhanced QOS-GNDA approach it find good node as well as recognize the selfish or the hidden malicious node. This approach may be extended in terms of to defend from impersonation attack.

REFERENCES

[1] Perkins Charles E., and Elizabeth M. Royer. "Ad-hoc on-demandDistance Vector Routing." Second IEEE Workshop on Mobile Computing Systems and Applications,Pp. 90-100. IEEE1999.

[2] Singh Umang, B. V. R. Reddy, and M. N. Hoda . "GNDA: Detecting Good Neighbor Nodes in Adhoc Routing Protocol." Second International Conference on Emerging Applications of Information Technology (EAIT), Pp. 235-238. IEEE 2011.

[3] T. Rajamohan Reddy, N. Sobharani. "Selective On-demand Protocol for Finding Reliable Nodes to form Stable Paths in ADHOC Networks."International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Pp-21-24, vol-1, no. 5, 2012

[4] Khatibi Sina, and Ruhollah Rohani. "Quorum-based Neighbor Discovery in Self-organized Cognitive MANET." 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Pp. 2239-2243. IEEE 2010.

[5] Biradar Rajashekhar and Sunilkumar Manvi. "Channel Condition and Mobility Based Choice of Neighbor Node for Routing in MANET." International Conference on Advances in Computer Engineering (ACE), Pp. 74-78, IEEE, 2010.

[6] Wang Gang, Shining Wu, Guodong Wang, Beixing Deng, and Xing Li. "Experimental Study on Neighbor Selection Policy for Phoenix Network Coordinate System." International Conference on ultra modern telecommunication, pp. 1-5. IEEE, 2009.

[7] Huang Yangcheng, Saleem Bhatti, and Soren-Aksel Sorensen. "Adaptive Neighbor Detection for Mobile Ad Hoc Networks." UCL department of Computer science,RN7:17.

[8] Sanchez Juan A., Pedro M. Ruiz, and Ivan Stojmenovic. "GMR: Geographic Multicast Routing for Wireless Sensor Networks." 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, vol. 1, Pp. 20-29. IEEE 2006.

[9] Moussa A. C., F. M. Kamel, D. Noureddine, and K. Maamar. "Integration of Dynamic Current Bandwidth Capacity Calculation for Existing AODV." International Conference on Information Technology and e-Services (ICITeS), Pp. 1-7, IEEE 2012.

[10] Narayanan Uma, and Arun Soman. "Bandwidth Efficient GNDA." IOSR Journal of Engineering (IOSRJEN) ,Vol. 3, Issue 6, Pp40-43 , 2013

[11]Pallavi Patil. “Good Neighbor Node Detection Technique In Manets Using QOSGNA”.International Journal of Innovative Research in Engineering & Management (IJIREM), ISSN: Volume-2, Issue-3, May 2015

[12] Obaidat, M.S.; Woungang, I.; Dhurandher, S.K.; Koo, V., "Preventing packet dropping and message tampering attacks on AODV-based Mobile Ad Hoc Networks," Computer, Information and Telecommunication Systems (CITS), 2012 International Conference on , vol., no., pp.1,5, 14-16May 2012.

[13]S. Mamatha and S. C. Sharma, “A highly secured approach against attacks in MANETs”, Intl. Journal of Computer Theory and Engineering, Vol. 2, No. 5, Oct. 2010.