ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Optimized Trust Model Baiting Scheme for Secure Communication

Kiran Krishnan[1], Aswathi Rajan[2]

Assistant Professor, Dept. of ECE, CAARMEL Engineering College, Pathanamthitta, Kerala, India[1]

PG Student, Dept. of ECE, CAARMEL Engineering College, Pathanamthitta, Kerala, India[2]

ABSTRACT: In Manet,the first demand is co-operative communication among nodes. The malicious nodes might cause security issues like grey holes and cooperative attacks. To resolve these attack issues,a planning Dynamic supply routing mechanism that is referred as cooperative bait detection theme (CBDS)integrates the advantage of each proactive and reactive defence design. In regional attacks, a node transmits a malicious broadcast informing that it's the shortest path to the destination, with the goal of intercepting messages.The malicious node will attract all packets by transmitting a Route Reply (RREP) packet to incorrectly claim that “fake” shortest route to the destination and then discard the received packets while not forwarding them to the destination. In grey hole attacks, the malicious node isn't abs initio recognized in and of itself since it turns malicious solely at a later time, preventing a trust-based security resolution from detecting its presence within the network. It then by selection, discards/forwards the information packets which undergo this process.We focus on detecting grey hole/collaborative region attacks by employing a dynamic supply routing (DSR)-based routing technique

KEYWORDS: Manet, grey hole,dynamic supply routing

I.INTRODUCTION

Analysis of the precise attack mechanism that evaluates misreporting channel condition is evaluated here. During this setting, a user will incorrectly report its channel condition as ‘over claiming’ (reporting its channel condition as higher than actual measurement). In a very mobile wireless network, mobile nodes will exert totally different channel conditions betting on their different locations. Once a node experiences a channel condition that is too poor to receive packets from a supply node, a third node might have an honest channel condition to receive each of the supply and also the destination information is distributed through that third node. The aggressor will increase its likelihood of relaying packets for the victim. During this system once a node become egoistic the information is distributed through another node and therefore varies the trail and thus decreases network performance by packet dropping and delay.

In this system once a node is detected as an egoistic node, some packet have by thenbe lost such that the network goes for one more path. Knowledge lost from egoistic node is extremely impossible to recover. The supply node once more sends request to all nodes and once more realizes another path for transmission thus seeking a replacement path whenever a miscalculation or an egoistic node is detected within the network. This might increase delay and overhead within the network and reduces network performance.

1.1 Cooperative Relaying

In a mobile wireless network, mobile nodes will have completely different channel conditions counting on their different locations. Once a node experiences a channel condition that is indisposed to receive packets from a supply node, a third node might have an honest channel condition from each supply node and therefore the supposed destination. Cooperative relaying network architectures facilitates a node that has poor channel conditions to route its packet through a node with an honest channel condition.To seek out such routes, a cooperative relaying protocol distributes channel condition information for every candidate path, selects the most applicable relay path, and supply incentives to inspire nodes to forward packets for different nodes.
The attacker’s goal during this simulation is to cut back the victim’s output. The wrongdoer will adopt two approaches. Within the conservative approach, the wrongdoer doesn't forward packets in place of the victim while not incorrectly reporting its channel condition. Within the aggressive approach, the wrongdoer over claims its channel condition so

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

that it increase its chance of relaying packets for the victim. Once a node underneath claims its channel condition, the node reduces its chance of being chosen for forwarding; the underneath claiming attack is therefore no worse than powering the node off. As a result, underneath claiming isn't a good attack against cooperative relaying. Through simulation, the impact of over claiming attack is evaluated. If the associate degree wrongdoer over claims its channel condition, the wrongdoer is a lot possible to be chosen because it isthe best candidate for relaying. Designating the wrongdoer as a relaying node provides the wrongdoer a chance to steal the packets or to adversely impact network performance.

All nodes have specific energy in a network, which helps them to transfer the information packets appointed ton them. But, once sure rate of transmissionsdecrease.During this, energy of a node determines whetherthe node is a egoistic one. They will even be outlined as nodes that don't forward others packets, therefore maximising their edges at the expense of others. Egoistic behaviour of nodes result in an avalanche of issues. These nodes aim to save lots of its resources. They discard the incoming packets which supported their individual energy, which ends in average end to finish delay. The behaviour of egoistic nodes results in decrease in overall knowledge accessibility of the network. The disadvantage of egoistic nodes square measure is thatit enjoys all the resources of a network.However it does not offer its own resources. It uses network resources like battery power for its own profit. The egoistic nodes make a network inactive. So the measure of degree of stinginess of nodes is incredibly vital.

II.RELATED WORK

[1] In this paper the author analyses specific attack mechanisms and states the consequences of misreporting channel condition on varied channel aware wireless network protocols as well as cooperative relaying protocols, routing metrics in wireless circumstantial network and timeserving schedulers. Here a secure channel condition estimation rule is proposed which will be wont to construct a secure channel-aware protocol in single hop settings and analyses the rule within the respects of performance and security, and performs a simulation study to know the impact of rule on system performance. The false channel condition reportsthe attacks introduced in this paper as troublesome to spot by existing mechanisms, since attacks are usually protocol compliant. Hence the channel condition menstruation mechanism has to be changed. Attack will therefore be performed by the wrongly victimised user who is illicitly registered to a network.

[2] In this paper, author introduces Janus, a framework for ascendible, secure, and economical routing for hybrid cellular and Wi-Fi networks. Janus uses an ascendible routing algorithmic rule with multiple channel access, for improved network outturn. Additionally, it provides protection against self-loving nodes through a secure crediting protocol and protection against malicious nodes through secure route institution and knowledge forwarding mechanisms. This paper value Janus by experimentation and show that its performance is eighty five percent of the optimum algorithmic rule, up with an element larger than fifty percent over previous work. This values the safety overhead of Janus against two varieties of attacks: less aggressive self-loving attacks and strictly malicious attacks.

[3] 3G cellular networks, like High Speed Downlink Packet Access (HSDPA) and Evolution knowledge Optimized (EV-DO), give broadband-like downlink speed to modify applications, like VoIP. The specification for 3G cellular knowledge services recommends implementing associate degree expedient computer hardware.Expedient computer hardware uses multiuser diversity the weakening and shadowing of cellular users inside one cell to optimize information measure potency. Each HSDPA associate degreed EV-DO use expedient computer hardware within the downlink to exploit multiuser diversity. To realize this goal, several networks need mobile devices to participate in managing network services. However, since mobile devices square measure outside the management of the network directors, networks shouldn't trust them to manage network operations. Sadly, this principle is commonly desecrated, as within the case of the favoured expedient planning algorithms, we tend to discovered 2 vulnerabilities:

(1) PF and TF schedulers trust channel condition reports from mobile devices while not verification.
(2) Both schedulers guarantee fairness solely inside one cell.

[4] In this paper author describes the planning and implementation of ETX as a metric for the Destination Sequenced Distance Vector (DSDV) and DSR (Dynamic supply Routing) routing protocols, moreover as modifications to DSDV and DSR which permit them to use ETX. Measurements taken from a twenty 9 node 802.11b test-bed demonstrate the poor performance of minimum hop count, illustrate the causes of that poor performance, and make sure that ETX improves performance. For long methods the outturn improvement is commonly an element of 2 or additional, suggesting that ETX can become additional helpful as networks grow larger and methods become longer.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

[7] In this paper implementation results show that the SUCAN system will give substantial performance will increase and protects against performance degradation even within the presence of malicious behaviour. trendy cellular knowledge services, like CDMA2000 (Code DivisionMultiple Access), adaptively opt for modulation schemes and writing rates supported the signal to noise quantitative relation between the bottom station and therefore the mobile user, permitting a lot of economical communications with mobile users that area unit nearer to the bottom station, whereas still providing lower-speed coverage to users that area unit farther removed from the bottom station.

III.SYSTEM ARCHITECTURE

The various components of the trust based model employed comprises of various modules.

1. Network Formation:
Here, formation of nodes occurs and the supply and destination nodes are chosen. When choosing the supply and destination nodes, supply desires to send the information to destination. Thus a route for information forwarding is needed.

2. Route Discovery:
Initially supply node broadcasts its route request according to the square measure of accessibility permissible. Neighbouring nodes receive the request and will check the destination address.If the actual node may be a destination it will generate route reply and send to supply through the corresponding path. If the node is not a destination it will forward to the next nodes. Once the route is chosen, all the nodes update their respective route caches.

3. Opinion Request Generation:
Whenever the supply node sends route request, it watches out for route reply. When obtaining the route reply it validates the route cache to detect entry of malicious nodes into the network. If negative, the supply node generates an opinion message and broadcasts to all neighbouring nodes. Here all the neighbouring nodes update messages if they sight any malicious nodes.

4. Update malicious node in Route Cache:
Source node updates malicious node in its route cache, it will not choose a specific path for data forwarding.
In this network formation we choose 50 nodes. Green nodes represents the source and destination nodes. Black colour node are intermediate nodes that are available in the network for packet transmission. Red node in the figure 1 indicate the malicious node entering the network.

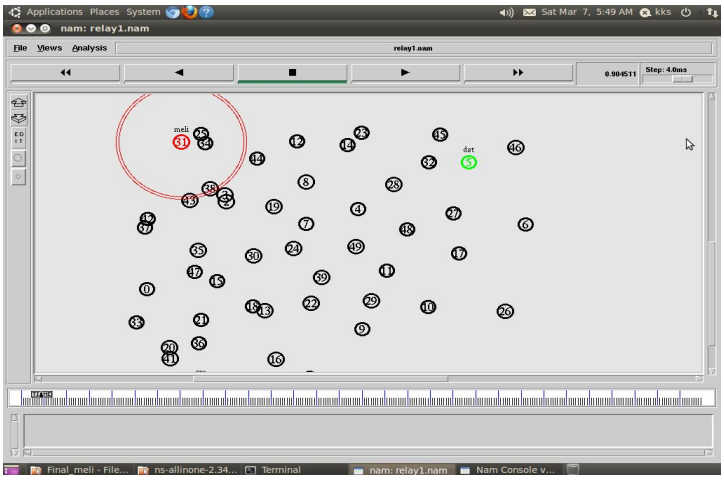

Fig.1: Entry of malicious node into the network.

The malicious node entering the network is shown in figure 1. While entering the network all the normal nodes will send the fake request to the node. Normally the fake node will reply but in some cases it will not reply for this request. To avoid this all the nodes will send the fake request to the malicious node. If any of the node detects any reply, it will broadcast to all the nodes in the network.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

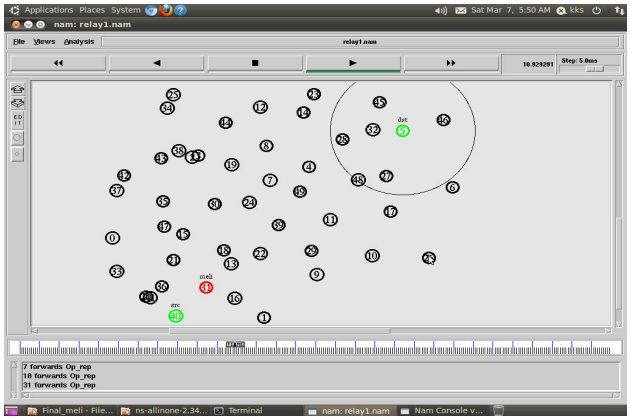

Fig.2: Malicious node in the network.

In figure 2 the malicious node has entered the network and all the nodes are checking and sending fake requests to the malicious node.

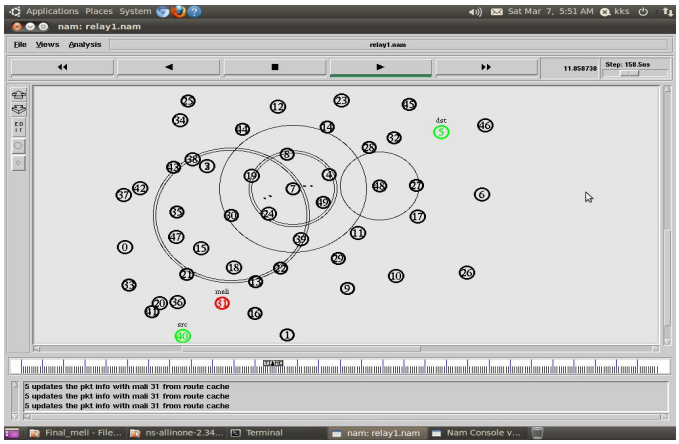

Fig. 3 : Malicious node identification.

In figure 3, the malicious node is identified by all nodes because of the broadcast message. Now all the nodes eliminate the malicious node from their route. They completely eliminates the path with the malicious node. Data is transmitted to the destination without any failure by avoiding the malicious node and path in the network.

IV. RESULT AND DISCUSSION

Using the trust value analyser, the source node gets trust values from both direct as well as indirect trust models as described in this paper. Using these trust values the hacker or malicious node is eliminated by the source node. An alternative path is selected for future communications. This model gives high anonymity protection. Besides that, the packet loss and delay diminishes by a fair measure and provides an overall better support for secure communication.

IV.CONCLUSION

In this paper the routing security issues of MANETs, are discussed. One type of attack, the black hole, which can easily be deployed against the MANET, is described. The percentage of packets received through the proposed method is better than that in AODV in presence of cooperative black hole attack. The solution is simulated using the Network Simulator and is found to achieve the required security with minimal delay & overhead. Future works may be concentrated on ways to reduce the delay in the network.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

REFERENCES

[1] Dongho Kim and Yih-Chun Hu, (2014), "A Study on False Channel Condition Reporting Attacking Wireless Networks", IEEE transactions on mobile computing, Vol. 13, No. 5, pp. 935-947
[2] Carbunar. B, Ioannis. I, and Nita Rotaru. C, (2009), "Janus: A framework for scalable and secure routing in hybrid wireless networks", IEEE transactions on Dependable Secure Computing, Vol. 6, No. 4, pp. 295–308.
[3] Dongbin Wang, Mingzeng Hu and Hui Zhi, (2008), "A survey of secure routing in ad hoc networks", The Ninth International Conference on Web-Age Information Management, IEEE DOI 10.1109/WAIM.2008.79.
[4] Douglas, De Couto D.S., Aguayo. J, Bicket. J, and Morris. R, (2003), "A high throughput path metric for multi-hop wireless routing", in Proc. ACM MobiCom, San Diego, CA, USA, pp. 134–146.
[5] Draves. R, Padhye. J, and Zill.B, (2004), "Comparison of routing metrics for static multi-hop wireless networks", in Proc. ACM SIGCOMM, Portland, USA, pp. 133–144
[6] Gaurav Soni and Kamlesh Chandrawanshi, (2013), "A novel defence scheme against selfish node attack in manet", International Journal on Computational Sciences & Applications (IJCSA), Vol.3, No.3, pp. 51-63.
[7] Haas. J. J, and Hu.Y. C, (2009), "Secure unified cellular ad hoc network routing" in Proc. IEEE Globecom, Honolulu, HI, USA.
[8] Hu. Y. C and Perrig. A, (2004), "A survey of secure wireless ad hoc routing" IEEE Security Privacy, Vol. 2, No. 3, pp. 28–39.
[9] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communication magazine,Vol.40, no.10, October 2002.
[10] C.E. Perkins, S.R. Das, and E. Royer, "Ad-Hoc on Demand Distance Vector (AODV)", March 2000.