PLACATE PACKET DROPPING ATTACK USING SECURE ROUTING PROTOCOL AND INCENTIVE BASED MECHANISM

M.V.S.S.Nagendranath[1], A.Nagajyothi[2], G.Phani Sindhuri[3]

[1]Assoc. Professor, Computer Science and Engineering, Sasi Institute of Technology and Engineering, Andhra Pradesh, India
[2]Student, Computer Science and Engineering, Sasi Institute of Technology and Engineering, Andhra Pradesh, India
[3]Asst. Professor Computer Science and Engineering, Sasi Institute of Technology and Engineering, Andhra Pradesh, India

Abstract

Ad-hoc networks are established voluntarily without the use of any framework or centralized management. This type of system infers that each node, or user, in the network can act as a data endpoint or intermediate node. Routing in between these nodes is established by using routing protocols. Several protocols for secure routing in adhoc networks have been proposed in the literature. But because of their drawbacks there is a necessity to make them strong and secure and these nodes are used to transfer the data from source location to destination. Whenever the nodes transfers data then the nodes has to utilize some resources like energy, storage capacity and bandwidth. So that some nodes of the network may not send data to their neighbor nodes. In this paper we use secure based routing protocol watchdog to identify misbehaving nodes and we propose incentive based mechanism to avoid selfish nodes in order to mitigate the packet dropping attack.

Keywords - *Adhoc Network, incentive based mechanism, packet drop attack, selfish node, Trust-Based routing*

----------***----------

1. INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires where the nodes transfers data from one location to another location. Because MANET is an example for spontaneous network the path between the nodes is established when necessary. After the path has established the mobile node transfers packet directly to the mobile node or through some intermediate nodes. In the process of transferring data packets through intermediate nodes some nodes may act as selfish nodes because the nodes will consume some resources while transferring the data.

There are number of routing protocols have proposed in the literature see [1], [2], [3] to detect selfish nodes. These protocols concentrate mainly on important issues like traffic load, mobility, and power requirements. Whereas trust based routing protocols see [4], [5], [6] are used to specify the trust value of a node by using certain mechanisms. So that these protocols will generate reliable and trustable route from source to destination node. In case if the path contains any selfish nodes then by using these routing protocols we can easily identify them. In this paper we concentrate on packet dropping attack and for this problem the solution is provided by using incentive based mechanism.

The remaining part of this paper is organized as follows. Section II represents the related work that has already been completed. Section III represents the packet dropping attack. Section IV represents Watchdog mechanism, Section V represents incentive based mechanism, and Section VI represents the proposed scheme. Finally, Section VII represents the conclusion of the paper.

2. RELATED WORK

In order to prohibit routing misbehavior in MANETs several solutions have been proposed previously. This section describes some of the routing protocols briefly.

CONFIDANT [4] is a trust based routing protocol which is used to identify the misbehaving node in the network. CONFIDANT protocol has four basic components. Those are Monitor, Reputation system, Path manger and Trust manager. Monitor is used to overhear the data. That means it specify whether the next hop node also forwarded the packet correctly or not. If it occurs any problem then it performs action by the reputation system. The Reputation system changes ratings of the problem caused node. If the rating of a node is less than certain threshold value then the node is treated as a malicious node and these ratings list are transferred to the Path manager. Finally Path manager selects the path by using these ratings. Trust manager is used to transfer warning messages to other nodes. CONFIDANT protocol is having following drawbacks

i. Managing friends list by trust manager is difficult.
ii. It can introduce false alarms.
iii. Choosing threshold value is difficult.

In Balakrishnan et al [7], introduce a TWOACK to inhibit selfishness in adhoc networks. TWOACK is an acknowledgement based schema. That means when a node sends a packet, the node's routing agent checks that the packet is received successfully or not by using this

approach. This is done by sending TWOACK packet back through the same path by receiver. In this process if the sender or intermediate node does not receive a TWOACK packet then this approach considers the next hop as a misbehaving node. The main drawback of this protocol is that it can't identify exactly which node is misbehaving node.

Muhammad Zeshan[8], proposed two-fold approach. In this it performs two different operations. One is detecting misbehaving node and second one is removing the misbehaving node. The sender sends a data packet to the destination through some intermediate nodes then the source has to receive acknowledgements from all the intermediate nodes. If the sender does not get the acknowledgement then the sender node again sends the packet through the same path. In this case also if sender does not receive the acknowledgement then the sender concludes that there is a misbehaving node in the network path. After this conclusion this approach performs second operation that is isolation. This is done by maintaining count of number packets sent and number of packets dropped. If the count of number of packets dropped for the particular node reached to certain threshold then that node is considered as misbehaving node. The pitfall of this approach is that it won't generate correct report regarding misbehaving nodes.

3. PACKET DROPPING ATTACK

One of the problems faced by MANET is packet dropping attack. A packet may be dropped by the nodes for several reasons. Those are

- Due to volatility of the medium.
- Due to shortage of energy resources.
- Due to save its resources.

In a network, packet dropping attack occurs as follows: When source node sends data to the destination through some intermediate nodes then any of the intermediate node may drop that packet without sending it to the neighboring node. Because if node sends packet to its neighboring then that particular node may lose some resources. So that some of the nodes in the network act as a malicious node. Because of this reason there is a chance to occur the attack called as packet dropping attack in the network. If the MANETs contain such attack then it put down the performance of the network. Because the data does not transferred to destination node. Below Fig 1 represents the packet drop attack.

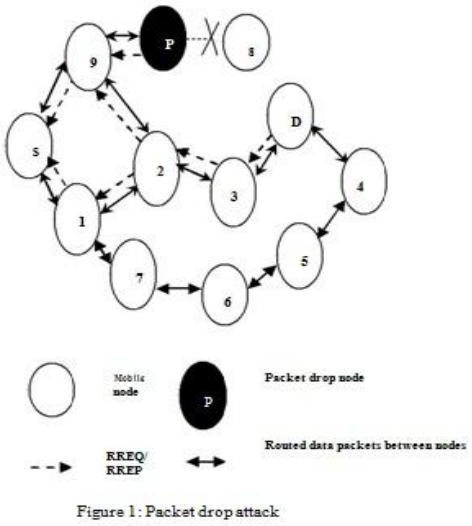

Figure 1: Packet drop attack

Fig 1: Packet dropping attack

4. WATCHDOG MECHANISM:

Watchdog [9] is a trust based routing protocol proposed by Marti et al and it is used to detect misbehaving node in a network. This mechanism maintains a buffer to store the transmitted packets and it performs overhearing operation. Then it compares overheard packet with the packet which is stored in the buffer. If both the packets are same then this mechanism clears that packet from the buffer. If the packet is placed in the buffer for more than an assertive period then the failure rate of the node (which does not forward the packet) will be increased. If the failure rate exceeds certain threshold value, it conclude that the node as misbehaving node and inform about this to source node.

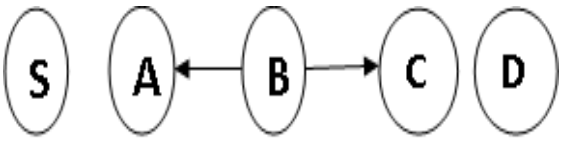

Fig 2: watchdog mechanism

Above diagram shows how watchdog mechanism works. There are five nodes in a path, node S is source and node D is destination and these two nodes will communicate with each other through the nodes A, B and C. In the above figure node A overhears the node B transmission. The line from B to C indicates that the source transferred data is transmitted from node B to node C. whereas line from B to A indicates that the node A overhears the B's transmission.

5. INCENTIVE BASED MECHANISM:

Butty´an and Hubaux proposed an incentive to cooperate by means of so-called nuglets [10].Incentive based mechanism is also called as credit based mechanism [10], [11], and [12]. This is used to prevent the network from selfish nodes. If the network contains selfish node then the packet dropping attack will occur. So that this model is used to avoid selfish nodes by including necessary credit in its packet by the source node. Each intermediate node takes required credit from the packet.

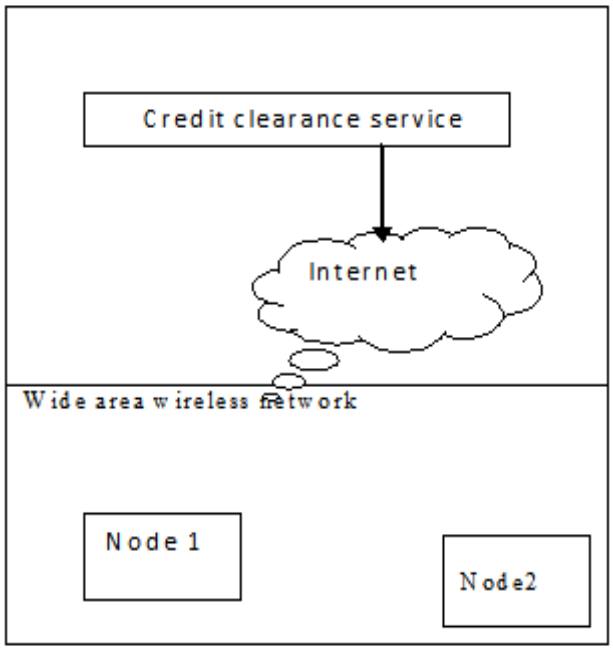

Fig 3: Architecture of SPIRITE

A node reports to the CCS, the messages that it has received/forwarded by uploading its receipts. If the intermediate node sends the packet to the neighboring node then it will get some credit which is sent by the sender.

For motivating nodes to forward packet, the CCS determines the last node on the path that has ever received the message. Then CCS asks the sender to pay β to this node, and α to each of its successors. Here α is considered to be one and β is a very small value (for eg: 0.01). Figure 4 illustrate the payment system. According to the scenario has taken in Fig 4, the sender pays a total of α+ β credits.

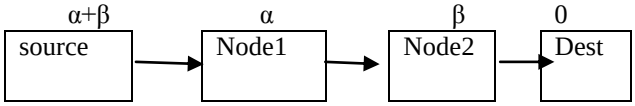

Fig 4: Illustration of payment system.

In this system there is a lot of burden on the source node because the source node has to credit to all the nodes in the path and another limitation is even though the node is not a selfish node, the sender has still accumulate the credit.

6. PROPOSED SCHEME:

In this section we present our solution to packet dropping attack by combining reputation and credit based approaches. Reputation based approach we considered here is watchdog. If we use the existing credit based approach then there is a lot of burden on the source node and also the source node will loss lot of credits. In order to solve this problem we propose a schema that whenever there is a selfish node then only the source node will accumulate the credit to the selfish node not for all the nodes in the network and that selfish node is identified by using reputation mechanism watchdog. This process is represented in the following Figure 5

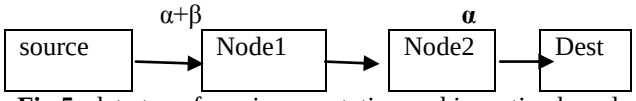

Fig 5: data transfer using reputation and incentive based mechanisms

Above figure shows the data transfer from source to destination after combining the two mechanisms(reputation and incentive). Initially the source will send the packet to destination through some intermediate nodes. The watchdog mechanism identifies whether the path contains any selfish nodes or not. If the path contains any selfish node then it sends message to the source node including the address of selfish node. Then the source node understood that the path contains selfish node and accumulate some credit to the address which is specified by the watchdog mechanism. That means the source will include credit to only selfish node in the path not for all the nodes. So that the source node can maintain number of credits. In the above Figure 5, the watchdog mechanism identified Node2 as selfish node and sends it address to source node. So that the source node accumulates credit α to Node2 only and maintain credit β at that node itself. Because of this mechanism burden on the will be reduced. The reduced overhead of the sender is shown in the Figure 6.

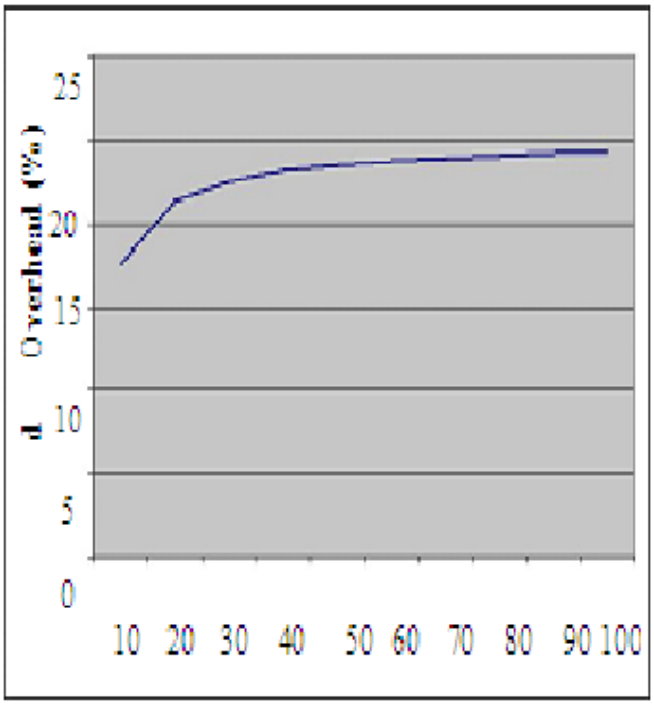

Fig 6: Reduced overhead (%) of sender

7. CONCLUSIONS

In this paper we combine reputation based mechanism and incentive based mechanism to avoid packet dropping attack. The solution is provided by identifying selfish node by using watchdog mechanism and after identifying, it is avoided by accumulating some credit to the selfish node by using incentive based mechanism. So that the source will not loss the large number of credits

REFERENCES

[1] Charles E.Perkins and Elizabeth M. Royer, "Ad hoc on demand distance vector (AODV) routing (Internet-Draft)", Aug-1998.

[2] L. M. Feeney, "A taxonomy for routing protocols in mobile ad hoc networks", Tech. Rep.,Swedish Institute of Computer Science, Sweden, October 1999.

[3] A.K. Gupta, Dr. H. Sadawarti and Dr. A. K. Verma, "Performance analysis of AODV, DSR & TORA Routing Protocols" in proceeding of IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010, ISSN: 1793-8236, pp. 226-231.

[4] S. Buchegger and J. Boudec, "Performance analysis of the confidant protocol: cooperation of nodes—fairness in distributed ad hoc networks," in Proc. IEEE/ACM Workshop Mobile Ad Hoc Networking and Computing (MobiHOC), pp. 226-236, 2002.

[5] T. Ghosh, N. Pissinou, and K. Makki, "Towards Designing a Trusted Routing Solution in Mobile Ad Hoc Networks," Mobile Networks and Applications, Springer Science, vol. 10, pp. 985-995, 2005.

[6] X. Li, M. R. Lyu, J. Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks". In the Proceedings of IEEE Aerospace Conference (IEEEAC) 2004, pp. 1286-1295.

[7] Selfishness in mobile ad h oc networks,". In The IEEE Wireless Communication and Networking Conference(WCNC'05), pp. 2137-2142, New Orleans,LA,USA, March 2005.

[8] Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema, Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks," International Seminar on Future Information Technology and Management Engineering 2008, pp. 568 – 572

[9] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad h oc networks," in Proceedings of the Sixthannual ACM/IEEE International Conference on M obile Computing and Networking, 2000, pp. 255–265.

[10] Crocraft, R. Gibbens, F. Kelly, S. Östring, Modeling Incentives for collaboration in mobile ad hoc networks, Performance Evaluation 57 (4) (2004) 427–439.

[11] L. Buttyan and J. P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Boston, MA, August 2000.

[12] M. Jakobsson, J.-P. Hubaux, L. Buttyan, A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks, in: LNCS, vol. 2742, Berlin, Heidelberg, Germany, 2004, pp. 15–33.