ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Enhanced Trust Based Bait Detection System for Mobile ADHOC Network

Madireddy Santoshdev
M.Tech,
Wireless & Mobile Communication
Farah Institute of Technology,
Chevella, R.R. Dist Telangana State,
India.

Anil Sooram
Associate Professor,
Department of ECE.
Farah Institute of Technology,
Chevella, R.R. Dist Telangana State,
India.

Dr.J.Sasi Kiran, Ph.D
Professor,
Department of ECE.
Farah Institute of Technology,
Chevella, R.R. Dist Telangana State,
India.

Abstract:

Our ultimate aim is to provide the high end detection method for gray-hole collaborative attack in MANET. Due to the widespread availability of mobile devices, MANETs have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks gray hole attack.

We propose a detection scheme called the cooperative bait detection scheme, which aims at detecting and preventing malicious nodes launching gray-hole/collaborative black-hole attacks in MANETs. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique.

Keyword:

Malicious node, Attack, cooperation, MANET.

1) Introduction:

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks.

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes them selves, i.e., routing functionality will be incorporated into mobile nodes. Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes.

In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network. A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. Protecting the mobile ad-hoc network from malicious attacks is very important and challenging issue. In this paper we address the problem of packet forwarding misbehavior and propose a mechanism to detect and remove the black and gray-hole attacks.

Fig.a Example Mobile-Adhoc Network

2) Related work:

In this [1] paper, the authors approach consisted of an algorithm which works as follows. Instead of sending the total data traffic at a time we divide the total traffic into some small sized blocks. So that malicious nodes can be detected and removed in between the transmission of two such blocks by ensuring an end-to-end checking. Source node sends a prelude message to the destination node before start of the sending any block to alert it about the incoming data block. Flow of the traffic is monitored by the neighbors of the each node in the route. After the end of the transmission destination node sends an acknowledgement via a postlude message containing the no of data packets received by destination node. Source node uses this information to check whether the data loss during transmission is within the tolerable range, if not then the source node initiate the process of detecting and removing malicious node by aggregating the response from the monitoring nodes and the network.

This Proactive detection schemes are schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of the existence of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted. In this [2] proposed a 2ACK scheme for the detection of routing misbehavior in MANETs. In this [2] scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received. A parameter acknowledgment ratio, i.e., Rack, is also used to control the ratio of the received data packets for which the acknowledgment is required. This scheme belongs to the class of proactive schemes and, hence, produces additional routing overhead regardless of the existence of malicious nodes.

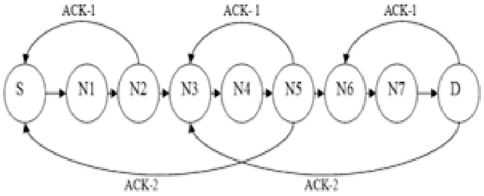

Fig.2 Example of ACK system

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead.

Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network. However, many research studies are working in energy harvesting to deal with this problemIn this article [3] author studied the routing security issues of MANETs, and analyze in detail one type of attack — the "black hole" problem — `that can easily be employed against the MANETs. Author also proposed a solution for the black hole problem for ad hoc on-demand distance vector routing protocol. One possible solution to the black hole problem is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node. Using this method the intermediate node cannot reply, so in some sense we avoid the black hole problem and implement a secured AODV protocol. But there are two associated disadvantages. First, the routing delay is greatly increased, especially for a large network.

Second, a malicious node can take further action such as fabricate a reply message on behalf of the destination node. And another method is considered in this paper, in that method the source node will verify the each next node information by forming the new route, but in this method, the overhead will increase and the security is not much better.Wireless ad hoc networks rely on multi-hop routes to transport data from source to destination. The routing function is implemented in a collaborative manner, with each node responsible for relaying traffic to the destination. However, an increasingly sophisticated pool of users with easy access to commercial wireless devices, combined with the poor physical and software security of the devices, can lead to node misbehavior.

A misbehaving node may refuse to forward packets in order to conserve its energy (selfishness), or simply degrade network performance (maliciousness). In this paper, we investigate the problem of uniquely identifying the set of misbehaving nodes that refuse to forward packets. We propose a novel misbehavior identification scheme called React that provides resource-efficient accountability for node misbehavior. React identifies misbehaving nodes based on a series of random audits triggered upon a performance drop.Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative black-hole attacks.

In existing research work, the author proposed a 2ACK scheme for the detection of routing misbehavior in MANETs. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received. A parameter acknowledgment ratio, i.e., Rack, is also used to control the ratio of the received data packets for which the acknowledgment is required. This scheme belongs to the class of proactive schemes and, hence, produces additional routing overhead regardless of the existence of malicious nodes.

3. Proposed solution:

This paper attempts to resolve collaborative black-hole attacks issue by designing a dynamic source routing DSR-based routing mechanism, which is referred to as the cooperative bait detection scheme that integrates the advantages of both proactive and reactive defense architectures. In our approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique.

3.1. Modules:

To improve our proposed work implementation, we have divided our proposed system into smaller modules.

- Design network
- Malicious node
- Legitimated node
- Co-operation checker
- Beacon generator
- Neighbor info Manager
- Route discovery
- FREQ generator
- RREQ/RREP processing
- Route maintenance

3.1.1 Network design:

In our project, we are mainly dealing with security side, to check our protocol strength we have to design the attacker and defender nodes. The attacker node able to check the route request and can give the fake reply to the source and attacker can identify the data packet and it will drop. Legitimated nodes can make the cooperation with neighbor and can make the communication, and forwards the data from one to other nodes, and can try to defend from attacker.

3.1.2 Cooperative checker:

In this module, we have used the timer to keep the time expire and intimates to generate the periodic packet. The beacon generator can generate the packet and that packet can be read by any neighbor node, the beacon life is only for one hop. The work of neighbor management unit is to store the neighbor information into a table when it receives the beacon packet from the neighbor. If the time is got expire the neighbor node info will be deleted from the table.

3.1.3. Route discovery:

Normally the source can find the route when the data is waiting in buffer without route by using the route request and route reply. In our project also we are going to use same method with different style, such as creating the fake route request.The source will generate fake request with destination address as cooperating neighbor. Source already knows the information, for Freq no reply. But incase if there is reply from any node, then that node will be identified as malicious by using the source routing mechanism.

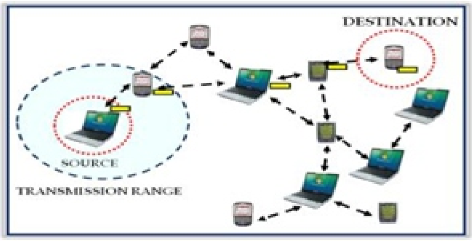

Fig.2 Routing in MANET

3.1.4 Route maintenance:

In this module, if route is failed means the intermediate node will share the error message. Based on the error message the source node will find another route to destination. With secure route discovery model .

3.2. Algorithm:

1)Initialize the Hello timer
2)If Hello timer expires

```
    a.Send hello message
3)If node has data
    a.If coop checking not yet over
        i.Get the random neighbor from table
        ii.Send the req to the neighbor node
    b.Else
        i.Send the req to destination
4)If packet received
    a.If the packet is hello packet
        i.If sender is not malicious
            1.If node is unknown node
                a.Add details in table
            2.Else
                a.Update the expire time

        ii.Else
            1.Ignore the packet
    b.If packet is Req packet
        i.Do basic packet filtering and updating operation
        ii.If current node is destination && sender is neighbor
            1.Set packet as Freq
            2.Ignore the packet
        iii.If current node is malicious node
            1.Send reply
        iv.If node is destination
            1.Send reply
    c.If packet is reply packet
        i.If current node is destination of reply packet && source is neighbor
            1.Set packet final node is malicious
            2.Ignore the packet
        ii.Else
            1.Do normal filtering and updating operation
```

3.3. Improved Coop-bait detection:

In our base work, the node checks the cooperation by sharing the neighbor information, in our enhancement work, we have introduced the technique to commited packet delivery checking process. The committed packet delivery system is nothing but each node has to count and compare the neighbor's packet with committed number of packets. If the received packet from neighbor is lesser than and committed packet of neighbor then neighbor will be identified as the malicious node.

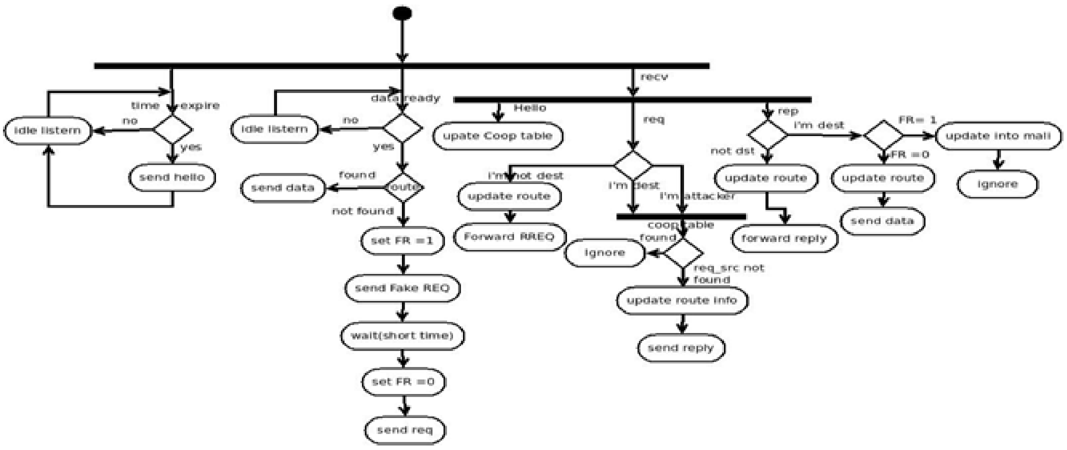

Fig.3 activity fo coop bait detection system

Result:

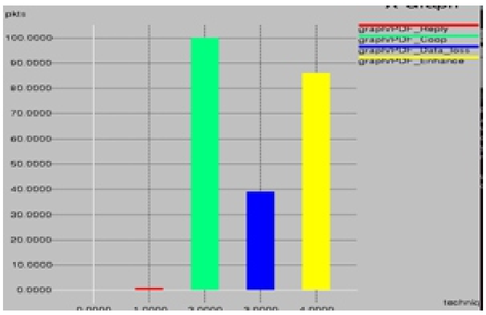

Fig. A PDF comparison.

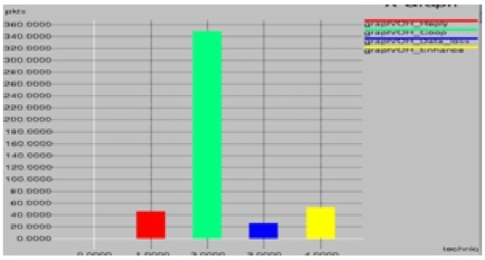

Fig. B overhead comparison.

Conclusion:

We have achieved our ultimate aim such as to provide the high end detection method for gray-hole collaborative attack in MANET. The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks gray hole attack. We proposed a detection scheme called the improved trust based cooperative bait detection scheme, which aims at detecting and preventing malicious nodes launching gray-hole/collaborative black-hole attacks in MANETs. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes detected using a reverse tracing technique. Our proposed system sucessfully tested with ns2. Energy factor is main important thinks in mobile adhoc network. So in our future work we will concentrate on then energy based attacks.

Reference:

1)"Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Sukla Banerjee, July 22, 2008.

2)"An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, May 2007.

3)"Routing Security in Wireless Ad Hoc Networks", Hongmei Deng, 2002.

4)"REAct:Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits", William Kozma Jr. 2009.

5)"Self-Organized Public-Key Management for Mobile Ad Hoc Networks, Srdjan Capkun, Levente Butty Ì n and Jean-Pierre Hubaux - 2003.

6)"ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks", Jiejun Kong, Xiaoyan Hong - 2003.

7)"Anonymous Secure Routing in Mobile Ad-Hoc Networks", Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng - 2004.

8)"ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks, Stefaan Seys and Bart Preneel - 2009.

9)"SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks", Azzedine Boukerche, Khalil El-Khatib, Li Xu, Larry Korba - 2004.

10)"ALARM: Anonymous Location Aided Routing in Suspicious MANET"s, Karim El Defrawy and Gene Tsudik - 2011.

11)"Identity-Based Encryption from the Weil Pairing", Dan Boneh, Matthew Franklin - 2001.

12)"SybilGuard: Defending Against sybil Attacks via Social Network"s, Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham Flaxman - 2006.

Author Details:

Madireddy Santoshdev Gratuated B.Tech in Electronic and communication Engineering in 2013 from Acharya Nagarjuna University . Presently, He is pursuing his Masters degree in M.Tech of Wireless and mobile communication in Farah Institute of Technology affiliated to JNTUH, Chevella, R.R. Dist Telangana State, India.

Anil Sooram Graduated in B.Tech ECE in 2007 from JNTU Hyd. He received Masters Degree in M.Tech [ECE] from JNTUH University, Hyderabad. Presently he is working as Associate Professor in ECE Dept. in Farah Institute of Technology, Chevella, R.R. Dist Telangana State, India. His research interests include Wireless Communications, Embedded Systems. He has published 3 research papers in International Conferences, Journals. He has received best Teacher award from Farah Group.

Dr. J.Sasi Kiran Graduated in B.Tech [EIE] from JNTU Hyd. He received Masters Degree in M.Tech [Computers & Communications] from Bharath University, Chennai, M.Tech [CSE] from JNT University, Hyderabad. He received Ph.D degree in Computer Science from University of Mysore, Mysore. He has served Vidya Vikas Institute of Technology for 10 years as Assistant Professor, Associate Professor, HOD-CSE&IT & Vice Principal and taught courses for B.Tech and M.Tech Students. At Present he is working as Professor in CSE and Dean – Academics in Vidya Vikas Institute of Technology, Chevella, Greater Hyderabad, R.R. Dist Telangana State, India.

His research interests include Image Processing, Cloud Computing and Network Security. He has published several research papers till now in various National, International Conferences, Proceedings and Journals. He is a life member of CSI, ACM, ISTE, IE, IAE, NSC, ISCA, IACSIT, CSTA, AIRCC, CRSI, GMIS-USA, Red Cross and Managing Committee Member of Computer Society of India. He has an editorial board member of IJERT and Board of Studies Member of CVSR Engineering College, Hyd. He has received Best Teacher award twice from Vidya Group, Significant Contribution award from Computer Society of India and Passionate Researcher Trophy from Sri. Ramanujan Research Forum, GIET, Rajuhmundry, A.P, India.