ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Secured Detection of Packet Dropping Attack in MANET

Ms.M.Divya[1] and Ms.D.Sasiya[2]
[1]*Assistant Professor and* [2]*M.Phil Scholar*
[1]divimsc.18@gmail.com and [2]yasisa.d1994@gmail.com
Department of Computer Science
Sri Adi Chunchanagiri Women's
College, Cumbum, Tamil nadu, India.

***Abstract*-- Mobility and portable nature of Mobile Ad hoc Networks (MANET) has increased its popularity by two fold. MANETs have become a commonly used network for various applications. But this advantage suffers with serious security concerns, mainly a wireless transmission medium perspective where such networks may be subject to packet dropping.Link error and malicious packet dropping are the two sources for packet losses in MANET. A node can act maliciously and could harm the packet sending process. The homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. The using protocol named secured Ad hoc on demand distance vector (SAODV), which can truthfully detect packet dropping attack in MANET. SAODV can detect malicious nodes by identifying dropping of routing and data packet. Packet dropping due to both link error and presence of malicious nodes can detect by SAODV. It also provides importance to preserve privacy of data.**

I. INTRODUCTION

In a multi-hop wireless network, nodes cooperate in relaying/ routing traffic. An adversary can exploit this cooperative nature to launch attacks. For example, the adversary may first pretend to be a cooperative node in the route discovery process. Once being included in a route, the adversary starts dropping packets. In the most severe form, the malicious node simply stops forwarding every packet received from upstream nodes, completely disrupting the path between the source and the destination. Detecting selective packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. Specifically, due to the open nature of wireless medium, a packet drop in the network could be caused by harsh channel conditions e.g., fading, noise, and interference, link errors, or by the insider attacker. In an open wireless environment, link errors are quite significant, and may not be significantly smaller than the packet dropping rate of the insider attacker. So, the insider attacker can camouflage under the background of harsh channel conditions. In this case, just by observing the packet loss rate is not enough to accurately identify the exact cause of a packet loss.

II. RELATED WORK AND BACKGROUND

Detecting selective packet-dropping attacks is more challenging in a highly mobile wireless environment. The main difficulty is the requirement that need not to only detect the node where the packet is dropped, but also identify whether the drop is intentional or unintentional. In order to precede a black hole attack, malicious node exploits the vulnerabilities of the AODV protocols which are generally designed with strong assumption of trustworthiness of all the nodes present in the network. Any node can easily misbehave and can make a severe harm to the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

network by targeting both data and control packets.Fig. 1 shows an example of a Black hole attack in MANET.

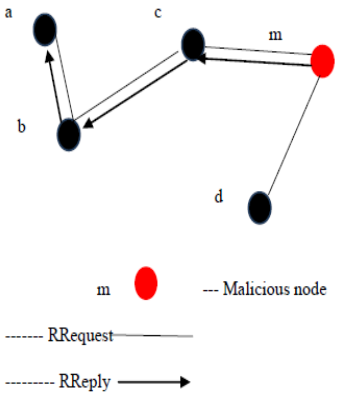

Fig. 1 Example of a Black hole attack in MANET

For making black hole attack malicious node should be in the routing path. Dropping of routing packets causes failure for source node to identify path to destination. Dropping of data packets leads to communication failure between nodes. Dropping of routing packets and data packets is an equivalent complex issue, so initial detection of malicious nodes are important for properdelivery of packets to destination. Link failures also have big part in packet dropping. In mobile wireless environment, link errors are quite significant, and shall not significantly smaller than the packet dropping rate of the malicious nodes.Fig. 2 shows an example of a Link failure.

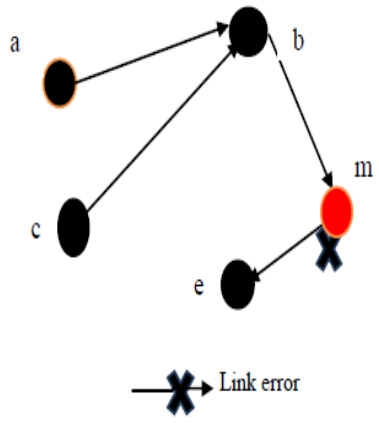

Fig. 2 Example of a Link failure

Here „m" is malicious and there is a chance for not forwarding the link failure information. Due to thissituation source node continue the packet sending through the same path a-c-m-e. Malicious node will drop all the packets coming through this path.

Packet Drop Attack

MANET consist of various kinds of attacks such as black hole attack, gray hole attack, packet drop attack, these all are a denial of service attack. In the black hole attack, a black hole node drops all the incoming packets by interpreting it as a valid shortest path. Ultimately destination node never receives any information from the source node. Hence, the performance of the network is compromised. In the packet drop attack, attacker node drops all packets that are passing through it as similar to black hole node, but difference is that it is not attracting neighbouring nodes to drop the packet.

In the packet drop attack, as malicious node does not attract neighbouring nodes to drop the packet, so it is less harmful to network than black hole attack. Packet Droppers are the malicious node that drops the packets routing through them.

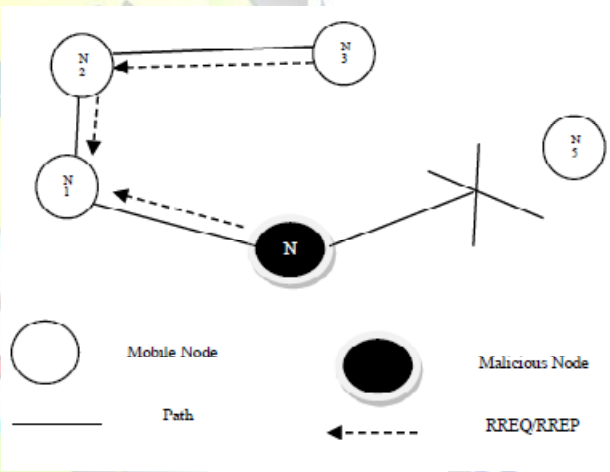

Fig. 3 Example of a performance of the symbols

Fig. 3 shows an example of a performance of the symbols. The detection technique of packet dropper node (Malicious Node) in MANET using SAODV theorem.

III. LITERATURE SURVEY

Tao Shu, Marwan Krunz.

"Detection of Malicious Packet Dropping in Wireless Ad Hoc Networks Based on Privacy Preserving Public Auditing"

Tao shu and Marwan krunz are interested in determining whether losses are due to link errors only

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

(or) due to the combined effect of link errors and malicious drops. To improve the detection accuracy, we propose to exploit the correlations between lost packets. To ensure the truthful calculation, they have developed a homomorphic linear authenticator (HLA) based public auditing architecture that allows to verify the truthfulness of the packet loss information reported by nodes. Using this architecture, it requires high computational cost and storage overhead.

P. Papadimitratos and Z. Haas,

" Secure message transmission in mobile ad hoc networks"

P. Papadimitratos and Z. Haas have described, in an open MANET environment, any node can maliciously (or) selfishly disrupt and deny communication of other nodes. They have used secure message transmission protocol which safeguards the data transmission against malicious behavior of another nodes. But it does not achieve end-to-end packet delivery.

Sirisha Medidi*, Muralidhar Medidi and Sireesh Gavini.

"Detecting Packet Mishandling in Mobile Ad-hoc Networks".

Sirisha Medidi, Muralidhar Medidi and Sireesh Gavini found that in a MANET, which is prone to security attacks, with node mobility being the primary cause in allowing security. For this purpose an unobtrusive monitoring technique to locate malicious packet drops. Using this makes the network to faults with packets getting misrouted (or) dropped.

Venkat Balakrishnan, Vijay Varadharajan, Uday Tupakula, and Phillip Lucs.

"Trust Integrated Co-operation Architecture for Mobile Ad-hoc Networks"

Venkat Balakrishnan, Vijay Varadharajan, Uday Tupakula, and Phillip Lucs, has been focusing on secure communications among nodes in MANET.To ensure this, trust model known as trust integrated co-operation architecture has been proposed. By using this model, we found that it either fail to protect against flooding attacks or only defend against greedy nodes that drops packets to save battery resources.

IV. ALGORITHM AND TECHNIQUE USED

Secure AODV Protocol Algorithm Analysis

The Secure Ad hoc On-Demand Distance Vector Routing Protocol (SAODV) is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation. SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). Route error messages are protected in a different manner because they have a big amount of mutable information. In addition, it is not relevant which node started the route error and which nodes are just forwarding it. The only relevant information is that a neighbour node is informing to another node that it is not going to be able to route messages to certain destinations anymore. Therefore, every node (generating or forwarding a route error message) uses digital signatures to sign the whole message and that any neighbour that receives verifies the signature.

- Vulnerability issues of AODV (due to intermediate nodes):
  - Deceptive incrementing of sequence number
  - Deceptive decrementing of hop count
- To secure AODV, approach 1 divided security issues into 3 categories:
  - Key Exchange
  - Secure Routing
  - Data Protection

Key Exchange:

- All nodes before entering the network procure a one-time public and private key pair from CA and CA's public key.
- After that, nodes can generate a Group Session Key between immediate neighbors using a suitable 'Group keying protocol'.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

- These session keys are used for securing the routing process and data flow.

Secure Routing (RREQ):

- Node **'x'** desiring to establish communication with **'y',** establishes a group session key $\mathbf{K_x}$ between its immediate neighbors.
- Creates RREQ packet, encrypts using $\mathbf{K_x}$ and broadcasts.
- Intermediate recipients that share $\mathbf{K_x}$ decrypt RREQ and modify.
- Intermediate nodes that do not share $\mathbf{K_x}$ initiate 'group session key exchange protocol' with the immediate neighbors.Fig. 4 shows an example of a Secure Routing (RREQ).

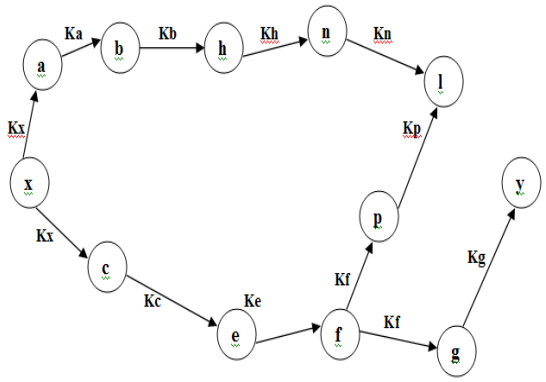

Fig. 4 Example of a Secure Routing (RREQ)

Secure Routing (RREP)

- In response to RREQ, **'y'** creates RREP.
- RREP is encrypted using the last Group session key that was used to decrypt RREQ and is unicast back to the original sender.
- If any of the intermediate nodes has moved out of wireless range, a new group session key is established.
- Recipient nodes that share the forward group session key decrypt RREP and modify.
- RREP is then encrypted using backward group session key and unicast to **'x'.**Fig. 5 shows an example of a Secure Routing (RREP).

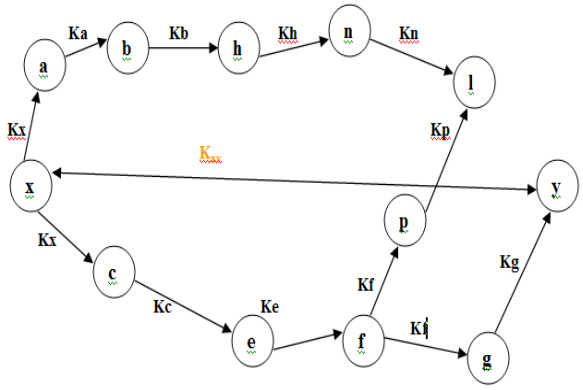

Fig. 5 Example of a Secure Routing (RREP)

Data Protection:

- Node **'x'** desiring to establish end-to-end secure data channel, first establishes a session key $\mathbf{K_{xy}}$with **'y'.**
- **'x'** symmetrically encrypts the data packet using $\mathbf{K_{xy}}$ and transmits it over the secure route.
- Intermediate nodes forward the packet in the intended direction.
- Node **'y'** decrypts the encrypted data packet using $\mathbf{K_{xy}}$.

This work deals with both routing and data packets dropping and also gives equal importance to identify link failures. This provides privacy for preserving truthful detection of packet dropping attack in MANET. Dropping can be due to presents of malicious nodes or due to link error.

Assumption:

M- Total number of nodes

Ni- Particular nodes

Ck- Particular cluster

Q- Maximum nodes possible in the cluster

P- Packet

Bi- Buffer

TCi- Trust counter (initially zero for every node)

TSi- Trust status (initially 'F' for every node) Th-0.8

Algorithm:

Step 1: Election of monitoring nodes

For (i-1 to M)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

```
                    {
Calculate node degree O;
Calculate power status O;
                }
While (every node is not in at least one cluster)
                {
If (Ni - - max (node degree and power status))
        {
        Add Ni into Ci
        }
  If (number of nodes in cluster > Q)
        {
        K++;
        }
```

Step 2: Detection of suspected nodes

```
        While (TSi < Th)
          {
    If (Ni forwarded packet P to node Nj)
        {
        Bi [Top] – Bi [Top] + P;
        Bi [Top +1] – Bj [Top];
         If (Bi [Top] - - Bi [top + 1])
              {
         Bi [Top] – Bi [Top] – P;
              }
                   Else
                      TCi – TCi + 0.2;
                          }
                  If (TCi > - Th)
                     {
                  Set TSi as 'S';
                  Go to step 3;
    }
```

Step 3: Process for suspected nodes

```
        Send Test RREQ to the node with TTL- 1
        If (response comes)
              {
                 TCi – TCi – 0.4;
              }
        Else
              Set TSi as 'D';
```

Step 4: Call DSR O;

Step 5: Verify path by the information of monitoring node.

This provides privacy for preserving truthful detection of packet dropping attack in MANET. Packet may be dropped during forwarding of routing information or during data forwarding. Dropping can be due to presents of malicious nodes or due to link error. SAODV can investigate the dropping and can find the malicious node or failed link behind this dropping. For identifying data packet dropping attack cryptographic scheme is added in SAODV.

V. CONCLUSION

Mobile Ad hoc Network (MANET) is a type of Ad-hoc Network which changes its location dynamically and configures itself. MANET does not have a fixed topology which causes priorities to different kind of attacks. In this work, it deals with detection and prevention of packet dropping attack. Link error and malicious packet dropping are two sources for packet losses in wireless ad hoc network. Work proposes a new protocol named SAODV which is different from HLA for security features. SAODV includes encryption scheme and checksum calculation. A coordinator node is introduced to manage all network operation. Coordinator is responsible for identifying packet dropping attack and find reasons for drop whether it is due to link error or due to the presence of malicious node. Coordinator can also perform corrective action against packet dropping.

REFERENCES

[1]. Tao Shu, Marwan Krunz. *"Detection of Malicious Packet Dropping in Wireless Ad Hoc Networks Based on Privacy Preserving Public Auditing"WiSec'12, April 16–18, 2012, Tucson, Arizona, USA.ACM 978-1-4503-1265-3/12/04 .*

[2]. Bobby Sharma Kakoty, S. M. Hazarika, N. Sarma. *"NAODV-Distributed Packet Dropping Attack Detection in MANETs ". International Journal of Computer Applications (0975 – 8887) Volume 83 – No 11, December 2013.*

*[3].*M. Kiran kumar, A. Sai Harish, *"A Novel Schema for Detecting Malicious Packet Losses". International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.5, Sep-Oct. 2012 pp-3633-3636.*

*[4].*P. Papadimitratos and Z. Haas,*" Secure message transmission in mobile ad hoc networks". Inter JRI Computer Science and Networking, Vol. 2, Issue 1, August 2010.*

[5]. Venkat Balakrishnan, Vijay Varadharajan, Uday Tupakula, and Phillip Lucs, *"Trust Integrated Co-operation Architecture for Mobile Ad-hoc Networks".*
ISSN: 0975-3397 Vol. 3 No. 7 July 2011 2601.

[6]. Haiyun luo, jiejun Kong, petros zerfos, songwu Lu, lixia zhang, "URSA: Ubiquitous and robust access control for mobile adhoc networks". To appear in IEEE/ACM Transactions on Networking, October 2004.

[7]. Sirisha Medidi*, Muralidhar Medidi and Sireesh Gavini, *"Detecting Packet Mishandling in Mobile Ad-hoc Networks".*
Volume 5, Issue 2, February 2015 ISSN: 2277 128X.

*[8].*R.Balakrishna, Dr.U.Rajeswara Rao" Video Conferencing over wireless ad hoc Networking", in Proc of Second International Conference on Cognation and Recognition, PES, Mandya, April 2008.

[9]. Er.Gurjeet Singh, "Performance and Effectiveness of Secure Routing Protocol in Manet", Global journal of computer science and technology 2012, Volume 12 Issue 5.

[10]. Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong and Joo-Han Song, "Experimental Comparisons between SAODV and AODV Routing Protocols", WMuNeP'05.

[11]. Djamel Djenouri and Nadjib Badache, "On eliminating packet droppers in MANET: A modular solution", Elsevier, AdHoc Networks (2009), Volume 7 Issue 6, Pages 1243- 1258.

[12]. S. Medidi, M. Medidi, S. Gavini, and R. Griswold. Detecting packet mishandling in Manets. In Security and Management, pages 159–162, 2004.

[13].R. Griswold and S. Medidi. Malicious node detection in ad-hoc wireless networks. In Proceedings of SPIE Aero Sense, Digital Wireless Communications V, April 2003.