ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Truthful Detection of Packet Dropping Attack in MANET

Noble George[1], Sujitha M[2]

Dept of Computer Science, Mangalam College of Engineering, M G University, Ettumanoor, Kottayam, India[1,2]

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. Mobility and portable nature of Mobile Ad hoc Network may also lead to link failure. During packet forward, valuable packets may be dropped by malicious nodes present in the network. 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. Ad hoc on demand distance vector (AODV) is a popular routing protocol but is exposed to well-known packet dropping attack. Proposed system introduces a new 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.

Keywords: MANETs, malicious nodes, link error, packet dropping.

I. INTRODUCTION

MANETs are a type of wireless networks which are rapidly growing because there is no such requirement for setting up an infrastructure for their operational purposes. In such networks, the topology is dynamic, and the nodes are mobile in nature. It must be able to continue their traffic even if the wireless transmission medium is out of range. This effectiveness and flexibility makes these types of networks attractive for many applications. Two nodes can communicate or send data packets to each other when they come within the radio range to each other, if they are not in the radio range neighbouring nodes forwards the packet to them. MANETs supports the multi hop communication between the nodes. While performing such operations, it may take into concern that the data cannot be dropped by malicious nodes or misbehaved links. It is still a challenging security concern [1].

Basic features of MANETs such as communication via wireless links, resource constraints cooperativeness between the nodes and dynamic topology make it easier to attack. Specifically in MANETs, one of very common attack is dropping data packets through malicious node.

In dropping data packet attack and routing packet attack malicious node prevents packets to forward to other mobile nodes and then drop these packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is equally important and cooperative. That means, if a node claims it can reach another node by a certain path or distance, then protocol takes the claim as real and similarly, when a node reports a link break, the link will not be used for next transmission.

AODV is the commonly used reactive routing protocol in MANET. It is an on-demand protocol, which initiate route request only when needed. AODV is also affected by packet dropping attack.

AODV performs better comparing to another protocol like dynamic source routing protocol (DSR) [13]. The proposed work adds security features to AODV and has introduced protocol named SAODV. Here it basically deals with packet dropping in network layer.

The first level of acknowledgment, such as Transmission Control Protocol Acknowledgment can detect end-to-end communication break, it is unable to identify accurately the malicious node which contributes that attack. Such mechanism is unavailable for connectionless transport layer protocols like User Datagram Protocol. Therefore, securing the basic operation of the MANET becomes one of the primary concerns in mobile environments in the presence of packets droppers [2]. The challenge lies in securing communication with the maintenance of connectivity between nodes under the crucial attacking situations and the frequently changing topology.

Packet Dropping Attack In AODV

A malicious node involved in a routing path may intentionally drop the packets at network layer in order to make a collapse in network performances. If particular malicious node intentionally drops all the forwarded packets going through that node it can be termed as black hole attack. Here it may also occur selective packet dropping, in this attack malicious node can selectively drop the packets originated from or destined to certain nodes that it not likes [4].

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

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

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 network by targeting both data and control packets [5].

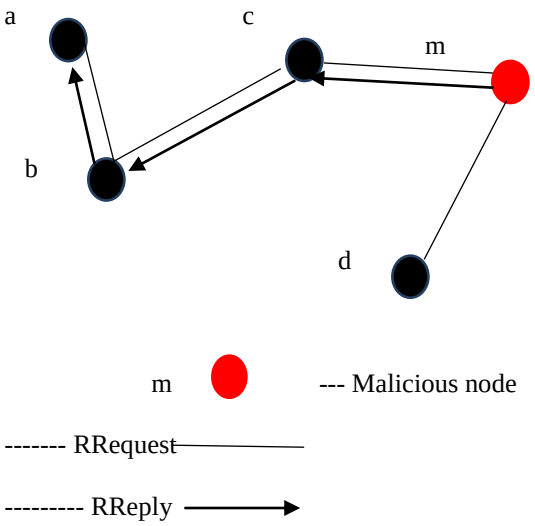

Fig. 1.Black hole attack in AODV

For making black hole attack malicious node should be in the routing path. Attack procedure can be explained as follows, as shown in Fig. 1, 'm' is a malicious node whereas 'a' and 'd' are the source and destination nodes respectively. Initially the source node 'b' broadcasts Route Request (RREQ) packet to its neighbours in one hop manner. After receiving this packet, each neighbour node is rebroadcasted if it has no route to destination. In this case malicious node 'm' may spoof the IP address of the destination 'd', inciting the source node 'a' to establish the path towards 'e', instead of 'd' or malicious node can claim that it has the shortest path to the destination and sends a RREP to source node 'a' . The source node 'a' realises that the route passing through the node 'm' is the shortest path, and thus it starts transmitting data packets towards 'm'. In both cases 'm' can drop all incoming packets or selected packets.

Dropping of routing packets causes failure for source node to identify path to destination. Source may conclude destination as unreachable. 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 proper delivery 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. .

Link failure is represented in Fig. 2, here link between 'm' and 'e' is broken. AODV protocol has option to inform neighbouring nodes about the link failure. In the given figure node 'e' informs malicious node 'm' about link failure between them via sending Route Error (RERR) message. Normal case node 'm' should inform neighbouring nodes about link failure and it will be forwarded to source node 'a'.

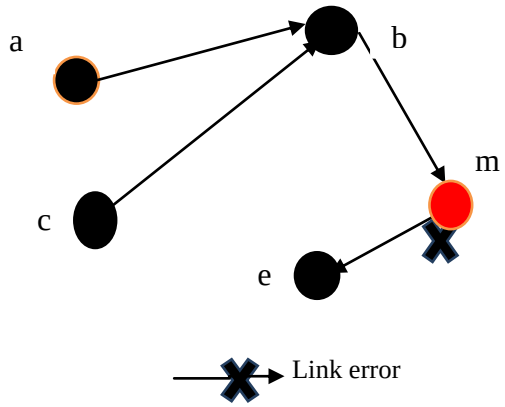

Fig.2. Link failure

Here 'm' is malicious and there is a chance for not forwarding the link failure information. Due to this situation 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.

Most of previous works only proposed the dropping due to link failure or due to malicious drops separately. In this work, protocol SAODV can handle these kinds of attacks and should take preventive actions against attacks that consider malicious nodes as the main cause of packet dropping but link failure also have equal part in packet dropping. Main focusing of existing works is to identify data packet dropping. This work deals with both routing and data packets dropping and also gives equal importance to identify link failures. The proposed system can take preventive actions too.

The rest of this paper proceeds as follows. In section II the related works are discussed. The SAODV protocol is discussed in section III. Section IV discusses the performance evaluation. Finally the proposal is concluded in section V.

II. RELATED WORK

Many researchers have been interested to develop several mechanisms to identify the malicious nodes that present in the routing path, and then to take control over data packets and routing packets.

To set up secured routing path, a new scheme is proposed in [10] within AODV. After the completion of normal path discovery procedure, the source node sends special control packets to get neighbour set of the node which have sent RREP packet. When it receives more than one reply, the node starts comparing the received neighbour sets. If the difference between them is larger than a threshold which is defined previously, then a black hole attack is identified. This method can reduce the chance of a successful black hole attack, but it cannot guarantee its prevention.

The authors of [11] have proposed a solution to the black hole attack in AODV. Here it suggests disabling the ability of an intermediate node to send a Route Reply (RREP)

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

message and allow only the final destination to do that. Work not proposed any authentication to RREP so an attacker can spoof the IP address destination node and it can act as the destination node. This may cause black hole attack.

A credit base system is proposed in [12], [16]. Credit system provides a credit score for cooperation between nodes. A node receives credit by forwarding packets for others, and uses its credit to send its packets to others. In this method, a malicious node may get enough credits by forwarding most of the packets it receives from upstream nodes, so selective packet dropping attack cannot be detected here.

Another work is based on reputation systems [13]. If a node have high packet dropping rate then its reputation given by its neighbours should be bad. This reputation information is propagated periodically throughout the network and it can be used as an important factor for selecting routes. The main drawback is that the malicious node can maintain a good reputation by forwarding most of the packets to the next hop, so it leads to consider malicious node as a normal node.

Some authors addresses the problem using cryptographic methods [6], [7],[8],[9]. For example, the work in [14], uses Bloom filters to make proofs for the forwarding of packets from each node. While the Bloom-filter scheme is able to provide a packet forwarding proof, the correctness of the proof is varying and there is a chance that it contain errors. In the case of detecting the selective packet dropping attack accuracy of this scheme is very low.

Hop-to-hop acknowledgements based approach is proposed in [10]. Acknowledgement based method used in this work only counts the number of lost packets, which does not give a sufficient ground to detect the real actor that is causing packet loss.
The proposed protocol SAODV considers dropping of both routing packet and data packets. It can identify the malicious node which causes the dropping.

III.SECURED AD HOC ON DEMAND DISTANCEVECTOR (SAODV) ROUTING PROTOCOL

In SAODV is proposed by adding additional security features to AODV. Which 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.

In this approach after identifying the source to destination path, all nodes included in the path should forward it's on public key to source node. Then the source node can encrypt the packet using public-key crypto-system such as RSA. Before the encryption process, the checksum value is calculated for the whole message. Message is then divided into packets. Each packet and its checksum is encrypted using RSA algorithm. Encryption is starting by using the public key of the destination node and end by the public key of nearest neighbour node of source. Checksum calculation is done by using MD5 algorithm [17].

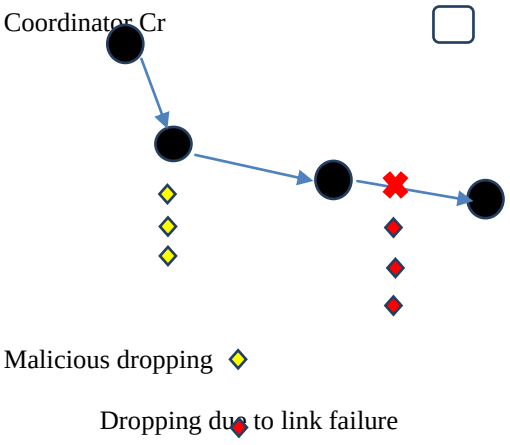

Fig.3.Network model

When packets reached at neighbouring node from source node it can decrypt it with its private key. It can decrypt only the part which is encrypted with its public key. Then packet and checksum is forwarded to next node in the routing path. Decryption and forwarding is done at each node until the targeted destination has reached. If decryption is not possible at any node it cannot allowed forwarding that packet. Each node should send acknowledgement to its upstream node regarding packet forwarding to next hope [15].

In the above case when decryption process is not done there is a chance that it is a malicious node, so it may drop the incoming packets. Here SAODV is not allowed to forward packet, so, no acknowledgement is received to upstream node that forwards the particular packets. After reaching threshold time if no acknowledgement has received in the upstream node from the downstream node, upstream node should inform coordinator node about acknowledgment lost.

There is an independent coordinator Cr in the network. Cr is independent of the routing path from source to destination and not involved in the path. It does not have any knowledge of the secrets like cryptographic keys held by various nodes. Before starting the packet transmission, source node should inform Cr about routing path. If checksum error occurred in the destination node, it will be informed to Cr.

When Cr receives message regarding acknowledgement loss from any node in the routing path, next is to identify reason for the packet loss. Here considered packet drops are due to presence of malicious node or due to link failure. Cr is responsible to identify whether it is link error or malicious drop. For this purpose each node need to send checksum of received packets and Cr compares it with

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

checksum received from source node. If any difference is present which means that the packet drop has occurred. During the next communication if same node fails in the checksum matching, it can be considered as a malicious and Cr will send warning message to source node. After receiving warning message from Cr, source node will remove particular malicious node from the routing path.

Black Hole Attack Detection

Each network node extracts the neighbours list from the received Hello messages and sends it to the Cr node. From this, Cr can construct network topology graph. When routing path is established between source and destination, the source node send path information to coordinator Cr. Upon reception of a message from the source node, the Cr extracts the number of neighbours claimed by the sender source node. Then it is compared with source node neighbour set calculated from the topology graph. This procedure is continued for all nodes in the routing path. If the difference between the claimed neighbours set and the one extracted from the graph exceeds the threshold which is defined previously, then the Cr node concludes that this is an attempt to make an attack and inform the source node to make new route.

Link Failure Identification

Link failures are also a main factor in packet dropping. Failed link need to be identified by coordinator Cr to prevent packet dropping. In SAODV each neighbouring nodes periodically send Hello messages to each other, absence of Hello message can be taken as an indication of link failure. It will be informed to Cr via neighbouring node of the failed link. By using this information Cr can inform source node to stop delivery from failed route. Then source node performs re-routing and identify new path to destination.

IV. PERFORMANCE EVALUATION

For comparing performance of AODV and SAODV ONE simulator is used. It is a java based simulation tool. Main focus is truthful detection of packet dropping attack. Two separate MANET is created for this purpose and one is simulated with AODV and another with SAODV. From this experiment it is identified that routing complexity of SAODV is higher than AODV, but proper detection of packet dropping attack can done by SAODV. As Compared to AODV, SAODV have very high detection rate. Experiment also shows that SAODV truthfully detect packet dropping attack in MANET.

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 AODV for security features. SAODV includes RSA based encryption scheme and MD5 based 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.

VI. ACKNOWLEDGEMENT

For the first, author would like to thanks all those people, who guided and supported. Taking this opportunity to express gratitude to all of the department faculty members for their help and support, and colleagues for their suggestions. And last but not the least, thank God.

REFERENCES

[1] TaoShu and Marwan Krunz, Fellow, IEEE. "Privacy-Preserving and Truthful Detectionof Packet Dropping Attacks in WirelessAd Hoc Networks," IEEE Transactions on MobileComputing, vol. 14, no. 4, April 2015

[2] B. Awerbuch, R. Curtmola, D.Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inform.Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

[3] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEEWireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[4] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle. Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs, In Proc. of the 33rd IEEE Conference on Local ComputerNetworks (LCN), Dublin, Ireland, October 2007.

[5] W. Yu, Y. Sun and K. R. Liu, HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks, In Proc. 24th IEEE INFOCOM, Miami, USA, March 2005.

[6] W. Mao, Modern Cryptography: Theory and Practice, Prentice Hall publisher, July 2005.

[7] A. Shamir, How to Share a Secret, Communications of the ACM, 22(11): 612-613, November 1979.

[8] L. Lamport, Password Authentication with Insecure Communication, Communications of the ACM, 24(11): 770-772, November 1981.

[9] A. J. Menezes, P. C. van Oorschotand S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, October 1996.

[10] H. Deng, W. Li and D. P. Agrawal, Routing security in wireless ad hoc networks, IEEE Commun. Mag., 40(10): 70-75, October 2002.

[11] B. Sun, Y. Guan, J. Chen and U. W. Pooch, Detecting black- hole attack in mobile ad hoc networks, In Proc. 5th European Personal MobileCommunications Conference, Glasgow, UK, April 2003.

[12] L. Buttyan and J. P. Hubaux, Nuglets: A Virtual Currency to Stimulate Cooperation in Self-organized Mobile Ad Hoc Networks, Swiss Federal Institution of Technology, Lausanne, Switzerland, Tech. Rep. DSC/2001/001, January 2001.

[13] M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup, and A. Menezes, PGP in constrained wireless devices, In Proc. 9th USENIXSecurity Symposium, Denver, Colorado, August 2000

[14] C. Perkins, E. Belding-Royer and S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, IETF RFC 3561 (Experimental), July 2003.

[15] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehaviour detection in wireless ad hoc networks," IEEE Trans. MobileComput., PrePrint, Vol. 99, published online on 6 Sept. 2013.

[16] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple cheat-proof, credit-based system for mobile ad-hoc networks," in Proc. IEEE INFO COM Conf., 2003, pp. 1987–1997.

[17] The MD5 Message-Digest Algorithm, RFC1321.