IMPACT: International Journal of Research in
Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 5, May 2014, 311-316
© Impact Journals

AN EFFICIENT CROSS LAYER APPROACH FOR MALICIOUS NODE DETECTION IN MANETs

ROSHAN KUMAR[1], MANEELA BHARDWAJ[2], SABA NAZ[3], MONA KUMARI[4], SRINIVAS N[5] & NALINI N[6]

[1,2,3,4]Department of Computer science & Engineering, Nitte Meenakshi Institute of Technology, Bangalore, Karnataka, India

[5]Assistant Professor, Department of Computer Science & Engineering, Nitte Meenakshi Institute of Technology, Bangalore, Karnataka, India

[6]HOD, Computer Science & Engineering, Nitte Meenakshi Institute of Technology, Bangalore, Karnataka, India

ABSTRACT

This paper presents a novel approach for Detecting malicious Node in MANETs. MANET is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. The main objective is to prevent MANETs from malicious node by using cross layer approach. Also we use encryption and decryption of data's that are to be transferred. Encryption is done at sender side and decryption takes place at the selected pop node. If decrypted data at the destination matches with the data that was sent by the server then only it is displayed at the pop node.

KEYWORDS: MANETs, Adhoc Network, Cross Layer, Malicious Node

INTRODUCTION

Ad Hoc Network is a method for wireless devices to directly communicate with each other. An example of an ad hoc network is given in Figure 1 where it allows all wireless devices to discover and communicate in peer –to –peer fashion without involving central access point. One of the best example is Bluetooth of a such networks. Any malicious node in the network can disturb the whole process or can even stop it. Several attacks like black hole, wormhole, rushing etc have been come into the picture under which a legitimate node behaves in a malicious manner. It is quite difficult to define and detect such behavior of a node. Therefore, it becomes mandatory to define the normal and malicious behavior of a node. Whenever a node exhibits a malicious behavior under any attack, it assures the breach of security principles like availability, integrity, confidentiality etc [4]. An intruder takes advantage of the vulnerabilities presents in the ad hoc network and attacks the node which breaches the security principles.

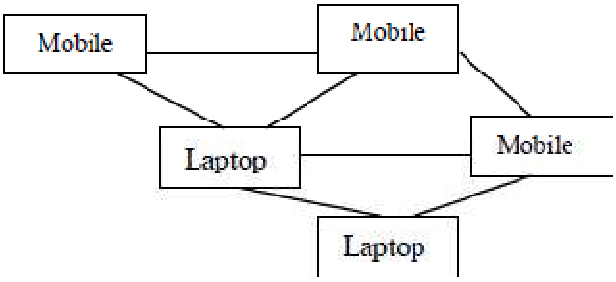

Figure 1: Example of Ad Hoc Network

BEHAVIOR OF NODES

Normal Behavior: The Process of delivering packets from source node (s) to destination node (D), while maintaining the basic requirements Availability (Av), Accessebility (Ac), and Authentications (Au), then It is called a Normal behavior of nodes.

Malicious Behavior: "When a Packet is Not delivered from source Node(s) to Destination Node (d), It comes under malicious behavior.

We can also detect malicious behavior if the following behavior occurs

- **Delay:** Malicious Node delay the Packets to forward from source(S) to destination (D).
- **High Bandwidth:** whenever nodes consumes high bandwidth, then it comes under malicious behavior.
- **Buffer Overflow:** It fills the Buffer with fake Updates so that it is unable to update genuine buffer.
- **Message Tampering:** Content of the packets may tamper.
- **Fake Routing:** Whether there exists a path between nodes or not, a malicious node can send fake routes to the legitimate nodes in order to get the packets or to disturb the operations.
- **Node Not Available:** An intruder can isolate the node from taking part in any operation so as to create delays when the source node chooses another alternative path.
- **Stealing Information:** Information like the content, location, sequence number can be stolen by the malicious node to use it further for attack.
- **Session Capturing:** When two legitimate nodes communicate, a malicious node can capture their session so as to take some meaningful information.
- **Others:** There are other ways also in which a node behaves in a malicious manner.

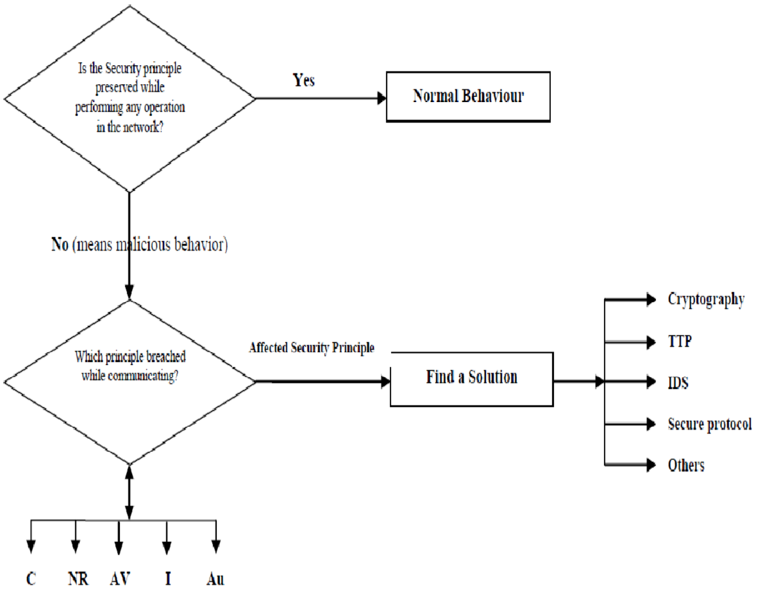
Is the Security principle preserved while performing any operation in the network?
Yes
Normal Behaviour
No (means malicious behavior)
Which principle breached while communicating?
Affected Security Principle
Find a Solution
Cryptography
TTP
IDS
Secure protocol
Others
C
NR
AV
I
Au

Figure 2: Defined Algorithm for Normal & Malicious Behavior of a Node

EXISTING SYSTEM

Watchdog

Marti et al. [17] proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. The Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

AACK

Sheltamiet al. proposed a new scheme called AACK. It is similar to TWOACK, It is a combination of a scheme called TACK and end-to –end-Acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The end-to-end acknowledgment scheme in ACK is shown in Figure 3. In the ACK scheme, as shown in below figure 3. The source node(s) sends packet and all intermediate nodes simply forward the packet, when the Destination nodes receives packet, It is requires to send back along the Reverse order. If the source node(S) receives the Ack packet, then packet transmission is successful, Otherwise it uses TACK scheme to sending TACK packets.

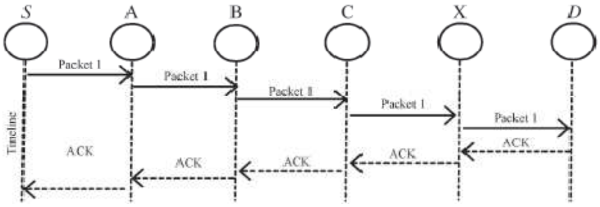

Figure 3: ACK Scheme: The Destination Node is Required to Send Acknowledgment Packets to the Source Node

PROPOSED SYSTEM

The main objective of this project is using on demand routing protocol, we can improve the Routing in MANETs. We use Route Request (RREQ) and Route Reply (RREP) concept to find the path between source and Destination.

The other concept is to find malicious Node.

When any node initiates a route discovery to another node, due to malicious behavior it may fails to forward the packets or it may fails to broadcast the Route Request (RREQ), it may happen to other Neigbhours also. Then communication between sender and receiver can not proceed.

In AODV routing Protocol, each node will sends hello message to obtain information from its neighbor, after Route request (RREQ) it forwards the packets to its neighbors.

After sometime, the node will monitor routing table to examine which nodes is unable to forward the packet and RREQ message. The node which is unable to forward the packets and RREQ is identified as malicious.

RELATED WORK

Node A wants to transmit a packet to node B. To do this, Awaits until the medium is free, requesting it by means of an RTS message (according to a transmission probability PTx). The message might, with probability PCOL, suffer from a collision if another node within the range of A sends an RTS at the same time. If there is no collision, node B replies with a CTS message, which can also collide with a probability PCOL if a hidden node, located within the range of B but out of range of node A, transmits some message at the same time. However, a CTS collision only happens if there is no previous RTS collision and, therefore, being the actual CTS collision probability (1 – PCOL)· PCOL. Once node A has accessed the medium, i.e. neither RTS nor CTS collision has occurred; it transmits the desired data to B, which will receive the packet unless a channel error happens. This occurs with probability PERR. Thus, B will receive the packet correctly only if there was no RTS collision, no CTS collision nor channel error.

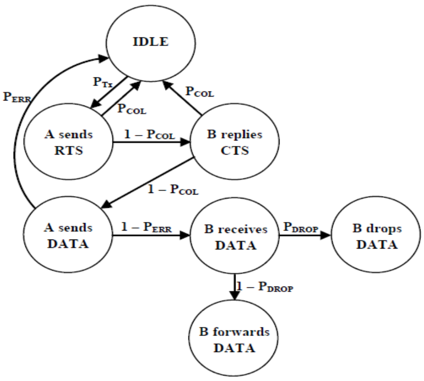

Figure 4: Flowchart for the Forwarding Process in MANETs

Working of AODV Protocol

AODV is a reactive protocol, i.e. routes to a given destination are established on demand. If a node needs a connection, it broadcasts a route request message (RREQ) that would be forwarded by other nodes. When a node receiving such a message has a route to the destination, it sends a route replay message (RREP) backwards. This whole process is known as route discovery.

In order to work properly, each node keeps track of the nodes it can communicate directly, considered as its neighbors, by listening for HELLO messages periodically broadcasted by each node. To avoid unnecessary bandwidth and energy consumption due to these messages, it is common in MANETs to use a link layer-based procedure to update the list of neighbors. When a node starts sensing the medium and sending RTS messages for relaying a packet, the procedure checks if the 802.11 RTS/CTS mechanism reaches the maximum number of retransmissions, i.e. the maximum number of RTS messages without a CTS reply. This value for RTS max is set to 7 by default in the protocol. In such a case, AODV considers that the link is broken and initiates a mechanism called route maintenance. Once the procedure starts, two possibilities may occur (Figure 4)

Node A wants to transmit a packet to node B. To do this, Awaits until the medium is free, requesting it by means of an RTS message (according to a transmission probability PTx). The message might, with probability PCOL, suffer from a collision if another node within the range of A sends an RTS at the same time. If there is no collision, node B replies with a CTS message, which can also collide with a probability PCOL if a hidden node, located within the range of B but out of range of node A, transmits some message at the same time. However, a CTS collision only happens if there is no previous RTS collision and, therefore, being the actual CTS collision probability (1 – PCOL)· PCOL. Once node A has accessed the medium, i.e. neither RTS nor CTS collision has occurred; it transmits the desired data to B, which will receive the packet unless a channel error happens. This occurs with probability PERR. Thus, B will receive the packet correctly only if there was no RTS collision, no CTS collision nor channel error.

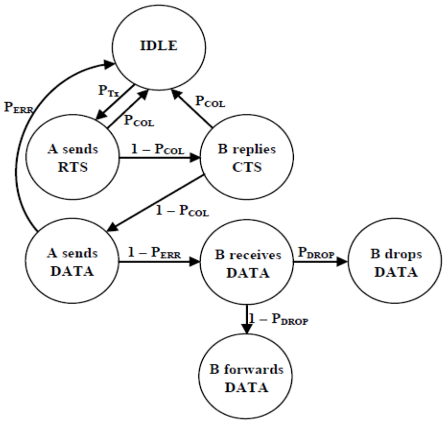

Figure 5: Flowchart for the Forwarding Process in MANETs

DATAFLOW DIAGRAM

A **data flow diagram (DFD)** is a graphical representation of the "flow" of data through an information system. DFDs can also be used for the visualization of data processing (structured design). On a DFD, data items flow from an external data source or an internal data store to an internal data store or an external data sink, via an internal process.

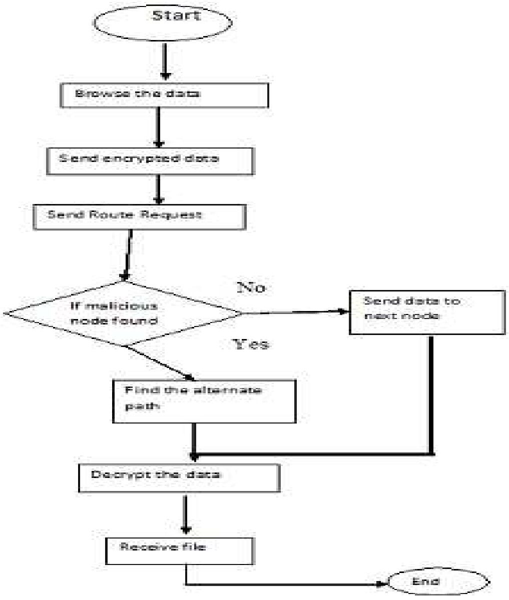

Figure 6: Flow Chart

CONCLUSIONS

This method gives a novel scheme to prevent MANETs from unauthorized access of data from malicious node that cannot reach destination node as well as data forwarded from source node is also encrypted. So the attacker cannot introduce himself as a source. Communication is not hampered between source and destination. Acknowledgment provides the details of the communication whether the message is reached or not. Due to the use of encryption and decryption, the transmission of data is more secure.

FUTURE ENHANCEMENTS

Here we consider MANETs in our simulation. This approach can be applied into VPNs as well as in VANETs. More type of files in advance to text and java files can be taken into consideration. We can also include the packet dropping detection with this method so probability of finding the malicious node will increase.

REFERENCES

1. Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami: "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

2. RekhaPatil, Shilpa Kallimath: "Cross Layer Approach for Selfish Node Detection in MANET", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 1, Issue 3, September 2012.

3. RadhikaSaini, ManjuKhari: "Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network", International Journal of Computer Applications (0975 ℵ8887) Volume 20, No.4, April 2011.

4. A. Rajaram, Dr. S. Palaniswami: "Malicious Node Detection System for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies, Vol. 1 (2), 2010, 77-85.

5. Martin Schütte: "Detecting Selfish and Malicious Nodes in MANETs", SEMINAR: SICHERHEIT IN SELBSTORGANISIERENDEN NETZEN, HPI/UNIVERSITÄT POTSDAM, SOMMERSEMESTER 2006.

6. Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathur and Prashant Khurana: "GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs", 27th International Conference on Advanced Information Networking and Applications Workshops 2013.