INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A SURVEY ON MANETS SECURITY: ISSUE, CHALLENGES AND SOLUTION

PROF. S. S. ASOLE[1], MISS. SHEETAL S. CHAVHAN[2]

1. Assistance Professor, Dept. of CSE, Babasaheb Naik college Of Engg., Pusad (India)
2. M. E. Student, Dept. of CSE, Babasaheb Naik college Of Engg., Pusad (India)

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes that form temporary network without aid of any existing network infrastructure or central access purpose. In contrast to the wire line networks, the distinctive characteristics of mobile ad hoc networks a cause variety number of nontrivial challenges to security design, such as open peer-to-peer specification , shared wireless medium, demanding resource constraints, and highly dynamic configuration. During this paper we identify the security issues related to this problem, and also discuss the challenges to security design, and review progressive security proposals that protect the MANET link-layer and network layer operations of delivering packets over the multi hop wireless channel. The complete security solution should span both layers.

Keywords: MANETs, security requirement, Security on routing, security issue, security challenges

PAPER-QR CODE

Corresponding Author: PROF. S. S. ASOLE

Access Online On:

www.ijpret.com

How to Cite This Article:

SS Asole, IJPRET, 2014; Volume 2 (8): 842-853

INTRODUCTION

In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. In this increasing quality of mobile device, like laptops, PDAs and handled digital devices, has motivated a revolutionary change in the computing world. We need to acquire information and connect to other device wherever we want. So it is necessary to adopt wireless because the as the interconnection method. A Mobile Ad hoc network (MANET) could be a is system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. A set of wireless mobile hosts dynamically establish their own network on the fly, while not looking forward to any preceding communication infrastructure. But this open network architecture and dynamic network topology are prone to be attacked internally and externally. that the final goal of the security solutions for MANET is to provide security services, like authentication, confidentiality, integrity, anonymity, and availability, to mobile users. It allows the devices to maintain connections to the network as simply adding and removing devices in the network. User has great flexibility to design such a network at least expensive and minimum time.

MANETs has shows distinct characteristics, such as:

- Weaker in Security
- Device size limitation
- Battery life
- Dynamic topology
- Bandwidth and
- slower knowledge.

MANETs has shows distinct security goals, such as:

- Authentication
- Integrity
- Confidentiality
- Non-Repudiation

2.**Basic Concepts**

Just kind of like wired network, the security service is to protect information and resources from attacks and misbehaviors. Here is widely used criterion to be met to confirm the Ad hoc network security:.

A mobile ad hoc network has following features:

A.Autonomous Terminal:

In MANET, every mobile terminal is associate autonomous node, which may function as both a host and a router. In other, since there's no background network words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. thus sometimes endpoints and switches are indistinguishable in MANET.

B. Distributed Operation

For the central management of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

C. Multi hop Routing

Basic types of ad hoc routing algorithms are often single-hop

and multi hop, supported totally different link layer attributes and Routing protocols. Single-hop MANET is simpler than multi hop in terms of structure and implementation, with the value of Lesser practicality and applicability. Once delivering data Packets from a source to its destination out of the direct Wireless transmission vary, the packets ought to forwarded Via one or more intermediate nodes.

D. Dynamic Configuration

Since the nodes are mobile, the configuration could modification apace and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions furthermore because the quality Patterns of the mobile network nodes. The mobile nodes in the Network dynamically establish routing among themselves as they move concerning, forming their own network on the fly.

E. Light-weight Terminal

In most cases, the MANET nodes are mobile devices with

Less CPU processing capability, small memory size, associate low power storage. Such devices would like optimized algorithms and Mechanisms that implement the computing and communicating.

3.ATTACKS

A MANET provides network connectivity between mobile nodes over potentially multihop wireless channels primarily through link-layer protocols that ensure one-hop property, and network layer protocols that extend the connectivity to multiple hops. These distributed protocols typically assume that all nodes are cooperative in the coordination process. This assumption is unfortunately not true in an exceedingly in a hostile environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers will simply disrupt network operations by violating protocol specifications. The main network-layer operations in MANETs are ad hoc routing and data packet forwarding, that move with one another and fulfill the practicality of delivering packets from the source to the destination. The ad hoc routing protocols exchange routing messages between nodes and maintain routing states at each node consequently.supported the routing states, data packets area unit forwarded by intermediate nodes along an established route to the destination. Nevertheless, both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. While a comprehensive enumeration of the attacks is out of our scope, such network-layer vulnerabilities typically fall under one in every of two categories: routing attacks and packet forwarding attacks, supported the target operation of the attacks. The family of routing attacks refers to any action of advertising routing updates that follow the doesn't specifications of the routing protocol.

The specific attack behaviors are related. to the routing protocol used by the MANET. For example, within the context of DSR [2], offender could modify the source route listed in the RREQ or RREP packets by deleting a node from the list, shift the order of nodes in the list, or appending a new node into the list [5]. once distance-vector routing protocols like AODV [1] are used, the attacker may advertise a route with a smaller distance metric than its actual distance to the destination, or advertise routing updates with a large sequence number and invalidate all the routing updates from alternative nodes [6]. By attacking the routing protocols, the attackers will attract traffic toward certain destinations in the nodes below their control, and cause the packets to be forwarded on a route that is not optimum or perhaps nonexistent. The attackers will produce can routing loops in the network, and introduce severe network congestion and channel contention in certain areas. Multiple colluding attackers could prevent a source node from finding any route to the destination, and partition the network within the worst case. There are still active analysis efforts in distinguishing and defeating a lot of refined and delicate routing attacks. for instance, the attacker may further subvert existing nodes in the network, or fabricate its identity and impersonate another legitimate node [7]. A combine of attacker nodes could produce a wormhole [6] and shortcut the normal flows between each other. In the context of on-demand ad hoc routing protocols, the attackers may target the route maintenance process and advertise that an operational link is broken [5].

3.1. Routing protocols

Routing in mobile ad hoc networks further issues and challenges in comparison when compared to routing in traditional wired networks with fixed infrastructure. There are several well-known protocols in the literature specifically are developed deal with the constraints obligatory by ad hoc networking environments. The problem of routing in such environments is aggravated by limiting factors like apace dynamical topologies, high power consumption, low bandwidth and high error rates. Most of the present routing protocols follow two different design approaches to confront the inherent characteristics of ad hoc networks, namely the table-driven and the source-initiated on-demand approaches. The following sections analyze in more detail these two design approaches, and in brief present example protocols supported them.

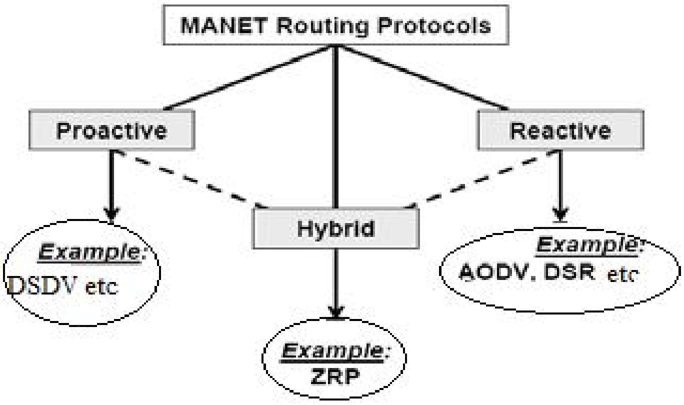

Fig. 1 Classification of MANET routing protocols

3.1.1) Proactive Protocols: Proactive, or table-driven routing protocols. In proactive routing, every node needs to maintain a lot of tables to store routing information, and any changes in configuration got to be reflected by propagating updates throughout so as to take care of a standardized network read . Example of such schemes is the conventional routing schemes: Destination sequenced distance vector (DSDV). They attempt to maintain consistent, up-to-date routing information of the whole network. It minimizes the delay in communication and permit nodes to quickly verify that which nodes are present or reachable in the network.

3.1.2) Reactive Protocols*:* Reactive routing is additionally referred to as on-demand routing protocol since they are doing not maintain routing information or routing activity at the network nodes if there's no communication. If a node desires to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery happens by flooding the route request packets throughout the network. Samples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV)[1] and Dynamic Source Routing (DSR).

3.1.*3)* Hybrid Protocols*:* They introduces a hybrid model that combines reactive and proactive routing protocols. The Zone Routing Protocol (ZRP) could be a hybrid routing protocol that divides the network into zones. ZRP provides a ranked design wherever every node needs to maintain additional topological information requiring further memory.

3.2. SECURE AD HOC ROUTING

The secure ad hoc routing protocols take the proactive approach and enhance the existing ad hoc routing protocols, like DSR and AODV, with security extensions. In these protocols, each mobile node proactively signs its routing messages using the cryptographical authentication primitives described above. This way, collaborative nodes will expeditiously demonstrate legitimate traffic and differentiate the unauthenticated packets from outsider attackers. However, an authenticated node may have been compromised and controlled by the attacker. Therefore, we have to further ensure proper compliance with the routing protocols even for an authenticated node. In the following, we describe how different types of routing protocols are secured.

Layer	*Security issues*
Application layer	*Detecting and preventing viruses, worms, malicious codes, and application abuses*
Transport layer	*Authenticating and securing end-to-end communications through data encryption*
Network layer	*Protecting the ad hoc routing and forwarding protocols*
Link layer	*Protecting the wireless MAC protocol and providing link-layer security support*
Physical layer	*Preventing signal jamming denial-of-service attacks*

Table 1. The security solutions for MANETs should provide complete protection spanning the entire protocol stack

3.2.1) Secure Link State Routing

(SLSP) could be a link state routing protocol for ad hoc networks. Its operations are similar to Internet link state routing protocols (e.g., Open Shortest Path First, OSPF): each node seeks to learn and update its neighborhood by Neighbor Lookup Protocol (NLP) and periodically floods Link State Update (LSU) packets to propagate link state information. NLP is responsible for:

1.1 Maintaining mappings between MAC and IP addresses of a node's neighbors

1.2 Identifying potential discrepancies, such as the use of multiple IP addresses on a single link

1.3 Measuring the control packet rates from each neighbor.

Neighbors use one-hop hello messages to discovery one another , and connectivity is assumed to be lost if a hello message is not received within a timeout. A node collects LSUs from all over the net- work in order to construct the global topology and calculate the route to any destination. Based on NLP, one LSU packet is constructed for each neighbor. Each LSU packet contains a sequence number and a hop count. Like DSR and AODV, duplicate LSU packets with previously seen sequence numbers are suppressed. The hop count determines the packet's time to live so that an LSU packet only travels within a zone, as in hybrid routing protocols like ZRP. An LSU receiving node adds a link to its global topology only if two valid LSUs from both nodes of the

link are received. Thus, one malicious node alone cannot inject false link information successfully. SLSP adopts a digital signature approach in authentication. NLP's hello messages and LSU packets are signed with the sender's private key. Any verifier can use the public key vouched for by the sender's valid certificate to verify a message's veracity. A certificate are often delivered to verifiers by either attachment to an LSU packet or dedicated public key disribution (PKD) packets. SLSP also employs various rate control mechanisms, such as time to live and rate throttle, in its NLP/LSU/PKD components. Thus, SLSP is less vulnerable to DoS attacks.

3.2.2. Secure Packet Forwarding

T he protection of routing message exchange is

only part of the network-layer security solution for MANET. It is possible for a malicious node to properly correctly participate within the route discovery phase but fail to correctly forward data packets. The security solution should ensure that each node indeed forwards packets according to its routing table.this is often generally achieved by the reactive approach because attacks on packet forwarding cannot be prevented: an attacker may simply drop all packets passing through it, even if the packets are carefully signed.

3.2.3. Other Routing Protocols

ARAN [7] ensures that every node knows the correct next mount on a route to the destination by public key cryptography. We illustrate the message exchange in ARAN using a simple example shown in Fig. 3. Each message is signed, and also the sender's certificate is attached to prove the authenticity of its public keys. A source S floods the network with a signed RREQ packet. Upon receiving the first copy of RREQ, a node sets up state of a reverse path, pointing to the node from which it receives the RREQ. It then signs and broadcasts the

packet. Upon receiving the RREQ, the destination D signs an RREP and uncast it back on the reverse path. Each node along the reverse path signs the RREP and sends it to the next hop, which verifies the signature of the previous hop, until S receives the RREP. Thus, the dis covered path is the one along which the first copy of RREQ reaches D from Seach node on this path knows the correct next hop, but not the whole path.

4. CHALLENGES

One fundamental vulnerability of MANETs Comes from their open peer-to-peer design. in contrast to wired networks that have dedicated Routers, every mobile node in an ad hoc network may function as a router and forward packets for alternative nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there's no clear line of defense in MANETs from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. There is no well defined place/infra- structure where we could deploy a single security solution.

Moreover, moveable devices, furthermore because the the system security information they store, are vulnerable to compromises or physical capture, particularly low-end devices with weak protection. Attackers may sneak into the network through these subverted nodes, , that cause the weakest link and incur a consequence of security breaches in the system.

The wireless medium and node mobility poses far more dynamics in MANETs compared to the wire line networks. configuration is extremely dynamic as nodes often be a part of or leave the network, and roam in the network on their own will. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay. Despite such dynamics, mobile users may request for anytime, anywhere security services as they move from one place to another.

The above characteristics of MANETs clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. First, the security solution should spread across many individual components and rely on their collective protection power to secure the entire network. The security scheme adopted by each device has to work within its own resource limitations in terms of computation capability, memory, communication capacity, and energy supply. Second, the security solution should span different layers of the protocol stack, with each layer contributing to a line of defense. No single-layer solution is possible to thwart all potential attacks. Third, the security solution should thwart threats from both outsiders who launch attacks on the wireless channel and network topology, and insiders who sneak into the system through compromised devices and gain access to certain system knowledge. Fourth, the security solution should encompass all three components of prevention, detection, and reaction, that work in concert to guard the system from collapse. Last but not least, the security solution should be practical and reasonable in an exceedingly extremely highly dynamic and resource- constrained networking scenario.

5. SOLUTIONS

5. 1 .Authentication during all phases

This solution consists of using authentication techniques during all phases, thereby excluding attackers or unauthorized nodes to participate within the routing. Most of the proposed solutions happiness to the present category modify existing routing protocols to create authentic ones [7]. They rely on Certificated Authority (CA) presence. as an example , the solution presented in [8] needs the utilization requires the use of a trusted certificate server whose public key is priory known to all valid nodes, this renders the solution centralized and less flexible.

5.2. Define new metrics: This metric is to be embedded into control packets to mirror the minimum trust value required by the sender, thereby a node that receives any packet can neither process it nor forward it unless it provides the required trust level presented in the packet. For this purpose, authentication is used to design SAR (Security-Aware Routing), a protocol derived from AODV and based on the trust values metric. In SAR, this metric is also used as a criterion to select routes when many routes satisfying the required trust value are available. To define nodes' trust values, authors address the example of military context, when trust level matches' to node's owner rank. however within the general context, wherever there's no hierarchy in the network, defining the nodes' trust values is problematic.

5.3. Secure neighbor detection

It consists of a three round authenticated message exchange between two nodes before each one claims the other as neighbor. If this exchange fails, then the well behaving node ignores the opposite, and doesn't handle packets sent by it. This solution beats the illegal use of high power range to launch the rushing attacks. Since the sender using higher powers cannot receive the packet from further nodes, it will not be able to perform the neighbor detection process, then their packets are unheeded by these nodes[2].

5.4. Randomize message forwarding:

This technique is proposed by [2] to to attenuate the prospect that a rushing adversary can dominate all returned routes. In traditional RREQ forwarding, the receiving node immediately forwards the RREQ and discards all subsequent RREQ. Using this scheme, a node collects a number of RREQs, and selects a RREQ at random to forward. There are thus two parameters to randomized forwarding technique: the quantity of REQUEST packets to be collected, and second, the algorithm by which timeouts are chosen. A detailed description is available in

[2].We think the drawback of this solution is that it increases the delay of route discovery, since each node must wait for a timeout or up to receiving a given number of packets before forwarding the RREQ. Moreover, the random selection prevents the invention of optimal routes, optimality is also in outline node hops variety , energy efficiency [2], or according to other metrics, anyway it is not random.

5.5. Information dispersal:

It consists of dispersing data over different routes. The source invokes the underlying route discovery protocol, and then determines an initial set of paths for communication with the specific destination, called APS (Active Path Set). so as to confirm high dispersal, it is preferable for these routes to be node-disjoint. With a set of routes at hand, the source disperses each outgoing message into a number of pieces. At the source, the dispersal introduces redundancy and encodes the outgoing messages. For this purpose, the algorithm proposed in [2] can be used, then each dispersed piece is transmitted across a different route. At the destination, a dispersed message with success reconstructed given that sufficiently a given number of pieces are received, in other words, the message dispersion ensures successful reception even if a fraction of the message pieces is lost or corrupted. A detailed description of the use of such a technique is available in [6, 2]

5.6. Use of feedback

To prevent data forwarding procedure from drooping attacks, feedback are often used. That is, the Destination validates the reception of packets by sending back cryptographically protected feedback or ACK to the source. the plain drawback with this solution is that it increases overhead.

5.7. Secure Message Transmission (SMT):

It [6] have proposed a protocol known as Secure Message Transmission which aims to Safe guard data transmission. . they need outlined and used all the solutions described above (End-to-end SA, Information dispersal, Use of feedback) to design SMT; a network layer protocol over routing protocol that aims to protect data transmission when operating above any multi route routing protocol. A full description of this solution is available in [6].

CONCLUSIONS:

In this paper we've studied the various MANET's security problems which the solutions developed for traditional networks area unit typically unsuitable during this Manet security surroundings. For the network layer we've conferred totally different forms of attacks on routing protocol and that we have classified and mentioned the projected solutions and connected challenges. we expect securing impromptu networks could be a nice challenge that has several opened issues of analysis, and receives a lot of and a lot of attention among manet networks community.

ACKNOWLEDGMENT

I express my thanks to **Prof. S. S. Asole** our guide for their kind co-operation and guidance for preparing and presenting this paper.

Last but not the least I would like to thank my entire friend who helped me directly or indirectly in my endeavour and infused their help for the success of this paper.

REFERENCES

1. Y. Hu, D. Johnson, and A. Perrig, “Sead: Secure Efficient, Distance Vector Routing for Mobile Wireless AdHoc Networks,” *IEEE WMCSA*, 2002

2. Gary Breed Editorial Director, “Wireless Ad-Hoc Networks: Basic Concepts”, High Frequency Electronics, March 2007

3. Priyanka Goyal, Vinti Parmar and Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011

4. Humayun Bakht, “ Survey of Routing Protocols for Mobile Ad-hoc Network”, International Journal of Information and Communication Technology Research, 258-270, October 2011.

5. Y.C. Hu, D.B. Johnson and A. Perrig, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” IEEE, Proceedings the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’02), 0-7695-1647-5, 2010.

6. P. Papadimitratos and Z. Haas, “Secure Link State Routing for Mobile Ad Hoc Networks,” IEEE Wksp. Security and Assurance in Ad Hoc Networks, 2003.

7. Mohit Kumar and Rashmi Mishra “An Overview of MANET: History, Challenges and Applications” , Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.