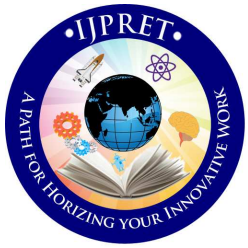
Research Article *ISSN: 2319-507X*
Ankur Mahalle, IJPRET, 2013; Volume 1(8): 632-639 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

APPROACH OF SECURE DATA TRANSMISSION IN MOBILE AD HOC NETWORKS

ANKUR S.MAHALLE[1], STEFFY H.POPLI[2]

1. Research Scholar, Department of Information Technology, PRMIT&R, Badnera, Maharashtra, India.

2. Assistant Professor, IBSS College of Engineering, Amravati, Maharashtra, India.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Security,
Reliability, Mobile Ad-hoc Networks (MANETs),
Routing protocols

Corresponding Author

Mr. Ankur S. Mahalle

Abstract

Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). However, its proliferation strongly depends on the availability of security provisions, among other factors. In the open, collaborative MANET environment practically any node can maliciously or selfishly disrupt and deny communication of other nodes. However, energy constrained nodes, low channel bandwidth, node mobility, high channel error rates, channel variability and packet loss are some of the limitations of MANETs. MANETs presents also security challenges. These networks are prone to malicious users attack, because any device within the frequency range can get access to the MANET. There is a need for security mechanisms aware of these challenges. Thus, this work aims to provide a secure MANET by changing the frequency of data transmission. The security of data transmission is achieved without restrictive assumptions on the network nodes trust and network membership, and at the expense of moderate multi-path transmission overhead only.

INTRODUCTION

Worldwide sales of smart phones, laptops, and PDAs have increased exponentially each year since their introduction. These mobile devices can be used to form MANETs. A MANET consists of arbitrary deployed communicational devices, such as cellular phones, Personal Digital Assistants (PDAs), laptop, etc. it is a multi-hop wireless network where all nodes cooperatively maintain the network connectivity. The mobile nodes are capable of connecting and communicating with one another using limited-bandwidth radio links. These types of networks are useful in any situation where temporary network connectivity is needed and in areas with no prefixed infrastructure, such as disaster relief where existing infrastructure is damaged, or military app

lications where a tactical network is required. In a wireless ad hoc network where pairs of mobiles communicate by exchanging a variable number of data packets along routes set up by a routing algorithm, reliability may be defined as the ability to provide high delivery rate, that is, to deliver most of the data packets in spite of faults breaking the routes or buffer overflows caused by overloaded nodes. Links failures may occur due to interferences on the wireless medium, or, most probably, to nodes mobility, when pairs of nodes move out of the reciprocal transmission range or are shadowed by obstacles. MANETs do not only provide dynamic infrastructure networks but also allow the flexibility of wireless devices mobility. MANETs differ significantly from existing networks. First, the topology of the nodes in the network is dynamic. Second, these networks are self-configuring in nature and do not require any centralized control or administration. Such networks do not assume all the nodes to be in direct transmission range of each other. Hence these networks require specialized routing protocols that provide self-starting behaviour. However energy constrained nodes, low channel bandwidth, node mobility, high channel error rates, and channel variability are some of the limitations of MANETs. Under these conditions, existing wired network protocols would fail or perform poorly.

Thus, MANETs require specialized routing protocols. To secure the data transmission phase, present here the secure message transmission (SMT) protocol, a secure end-to-end data forwarding protocol tailored to the MANET communication requirements. SMT safeguards the communication across an unknown, frequently changing network in the presence of adversaries that exhibit arbitrary malicious behavior. The goal of SMT is not to securely discover routes in the network the security of this phase should be achieved by protocols such as the secure routing protocol (SRP). The goal of SMT is to ensure secure data forwarding, after the discovery of routes between the source and the destination has secure data forwarding, after the discovery of routes between source and the destination has been performed.

In other words, SMT assumes that there is a protocol that discovers routes in the ad hoc network, although such discovered routes may not be free of malicious nodes

An illustrative example of a single message transmission is shown in Fig. 1. The sender disperses the encoded message into four packets, so that any three out of the four packets are sufficient for successful reconstruction of the original message. The four packets are routed over four disjoint paths and two of them arrive intact at the receiver. The remaining two packets are compromised by malicious nodes lying on the corresponding paths; for example, one packet is dropped, and one (dashed arrow) is modified.

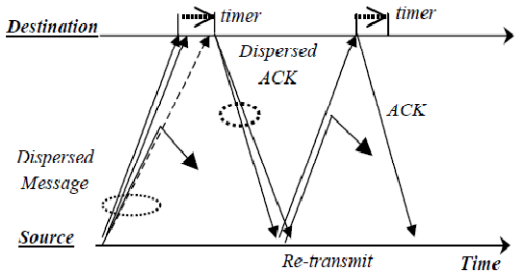


Figure 1. Simple example of the SMT protocol.

The receiver extracts the information from the first incoming validated packet and waits for subsequent packets, while setting a reception timer. When the fourth packet arrives, the cryptographic integrity check reveals the data tampering and the packet is rejected. At the expiration of the timer, the receiver generates an acknowledgement reporting the two successfully received packets and feedbacks

the acknowledgment across the two operational paths.

I. LITURATURE REVIEW

MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalable. A Mobile Ad hoc Networks (MANETs) is collection of mobile node communicating each other in the absence of any infrastructure while Vehicular Ad hoc Networks (VANETs) represents a class of MANET. The main advantages of MANET include easy deployment, distributed control, bandwidth efficiency and no need for infrastructure[1].

In any network, the sender wants its data to be sent as soon as possible in a secure and fast way, many attackers advertise themselves to have the shortest and high bandwidth available for the transmission such as in wormhole attack, and the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between the nodes

To secure the data transmission phase, here the secure message transmission (SMT) protocol, a secure end-to-end data forwarding protocol tailored to the MANET communication requirements. The SMT protocol safeguards pair-wise communication across an unknown frequently changing network, possibly in the presence of adversaries. It combines four elements: end-to-end secure and robust feedback mechanism, dispersion of the transmitted data, simultaneous usage of multiple paths, and adaptation to the network changing conditions. SMT requires a security association (SA) only between the two end communicating nodes, the source and the destination. Since a pair of nodes chooses to employ a secure communication scheme, their ability to authenticate each other is indispensable.

SMT is capable of delivering up to 250% more data messages than a protocol that does not secure the data transmission. Moreover, SMT outperforms an alternative single-path protocol, a secure data forwarding protocol we term Secure Single Path (SSP) protocol. SMT imposes up to 68% less routing overhead than SSP, delivers up to 22% more data packets and achieves end-to-end delays that are up to 94% lower

than those of SSP. Thus, SMT is better suited to support QoS for real-time communications in the ad hoc networking environment. The security of data transmission is achieved without restrictive assumptions on the network nodes' trust and network membership, without the use of intrusion detection schemes, and at the expense of moderate multi-path transmission overhead only.

As for security solutions targeting MANET data transmission, the use of multiple routes existing in multi-hop topologies has been proposed in the early work of and then in. From a different perspective, it has been proposed to detect misbehaving MANET nodes and report such events to the rest of the network. All the network nodes maintain a set of metrics reflecting the past behavior of other nodes and then select routes through relatively well-behaved nodes . A more recent work , makes the additional provision that all nodes have a secure association with all other network nodes. Thus, they can authenticate the misbehavior reports they exchange with their peers, seeking to detect and isolate malicious nodes that do not forward data packets. Another method to detect an attacker lying on the utilized route has been proposed in [4]. Once the communication across the route experiences a loss rate beyond a tolerable threshold, the source node initiates a search along the route to determine where the failure occurred. To do so, an encrypted and authenticated dialogue is initiated with each node along the route, with all network nodes assumed being securely associated with all their peers. Finally, a different approach provides incentive to nodes, so that they comply with protocol rules and properly relay user data. The assumed greedy nodes forward packets in exchange for fictitious currency.

II. SECURE MESSAGE TRANSMISSION

3.1 Message Dispersion and Transmission

The information dispersal scheme is based on Rabin's algorithm [3], which acts in essence as an erasure code: it adds limited redundancy to the data to allow recovery from a number of faults. The message and the redundancy are divided into a number of pieces, so that even a partial reception can lead to the successful re-construction of the message at the receiver. In principle,

the encoding (and dispersion) allows the reconstruction of the original message with successful reception of any M out of N transmitted pieces. The ratio r = N/M is termed the redundancy factor.

3.2 Determination of the APS

SMT can operate with any underlying routing protocol, although the use of a secure protocol is essential to reap the benefits of SMT. With SMT, at any particular time, the two communicating end nodes make use of a set of diverse, preferably node-disjoint paths that are deemed valid at that time. We refer to such a set of paths as the Active Path Set (APS). The source first invokes the underlying route discovery protocol, updates its network topology view, and then determines the initial APS for communication with the specific destination. Otherwise, adversaries could disable communication by continuously providing false routing information. SMT is independent of the route discovery process – for example, it can operate in conjunction with a reactive or a proactive protocol. However, the knowledge of the actual nodal connectivity and the use of source routing result in two advantages. First, it is possible for the sender to implement an arbitrary path selection algorithm in order to increase the reliability of the data transmission. For example, the path selection algorithm could incorporate subjective criteria, such as nodes to be explicitly included or excluded from the APS. Second, no discretion on route decisions is left to intermediate nodes, in order to enhance the robustness of the protocol. This way, the communicating end nodes can explicitly correlate the failed or successful transmissions with the corresponding routes. As a result, non-operational and possibly compromised routes are unambiguously detected at the source node, so that newly determined routes can be entirely different from previously utilized and discarded routes. For the rest of the paper, we assume that a secure routing protocol provides a number of routes to SMT, every time the route discovery protocol is executed.

III. APPROACH

4.1 The security approach

There are two main categories of routing protocol in MANET (figure): proactive and reactive Proactive protocols maintain fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. Reactive protocols find a route on demand (only when needed) by flooding the network with Route Request packets.Reactive protocols also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. These protocols setup routes when demanded. When a node wants to communicate with another node in the network, and the source node does not have a route to the node it wants to communicate with, reactive routing protocols will establish a route for the source to destination node. In proactive protocol, when a new node is added in the network it takes some time to converge during that time if we want to send data to destination through that new node immediately, it takes some time to converge and then it will transmit the data. To avoid this problem we are going to use reactive protocol instead of proactive in that time that is until network converge [5].

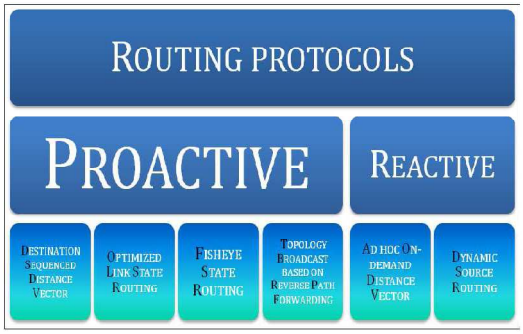


Figure2. Routing protocols classification

The Secure Single Path (SSP) protocol is the limiting case of SMT without the dispersion of outgoing messages and the use of a single path for each message transmission. SSP is equipped with the same end-to-end feedback and the fault detection mechanisms as SMT. SSP also re-transmits each failed message $Retry_{max}$ times, provides data integrity, authenticity, and replay protection as SMT does, and selects the shortest path in hops. SSP determines, utilizes, and maintains a single path only. Once the utilized path is deemed failed, a new route discovery may be needed in order to determine a new route.

4.2The mobility aware approach

If the motion parameters of two neighboring nodes like speed, direction, radio propagation range are known, the duration of time these two nodes will remain connected can be determined.

IV. CONCLUSION

The SMT and SSP protocols for secure data communication in ad hoc networks. The two protocols are widely applicable, as they provide lightweight end-to-end security services, and operate without knowledge of the trustworthiness of individual network nodes. They are highly effective, achieving highly reliable, low-delay, and low-jitter communication even in highly adverse settings.

SMT and SSP are versatile, as they automatically adapt their operation to resource constrained environments, as well as application requirements. In fact, our protocols span a large space of solutions, offering the flexibility to trade off overhead for enhanced fault-tolerance and reliability, or trade off delay and delay variability for low overhead. For future work we intend experimenting the changing frequency approach combined with the proposed mobility aware approach, using more metrics and criteria (such as nodes energy, mobility, connectivity, vicinity, etc.).

REFERENCES

1. Saurabh Singh, Dr. Harsh Kumar Verma , "Security For Wireless Sensor Network", International Journal on Computer Science and Engineering, Vol. 3 No. 6 June 2011.

2. H.L.Nguyen,U.T.Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks,” International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.

3. P. Papadimitratos, Z.J.Haas, and E.G.Sirer, “Path Set Selection in Mobile Ad Hoc Networks,” in proceedings of the Third ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc 2002), Lausanne, Switzerland, Jun. 2002.

4. P. Papadimitratos, Z.J. Haas, and P. Samar, “The Secure Routing Protocol (SRP) for Ad Hoc Networks,” Internet Draft, draft-papadimitratos-secure-routing-protocol-00.txt, Dec. 2002.