ISSN: 2321-7782 (Online)
Volume 3, Issue 3, March 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Improvised Mobile Web for Secure Data Transmission

Rupesh M. Hushangabade[1]
Information Technology Department
Prof. Ram Meghe Institute of Technology & Research,
Badnera-Amravati, India

Abhishek A. Gulhane[2]
Information Technology Department
Prof. Ram Meghe Institute of Technology & Research,
Badnera-Amravati, India

Smeet D. Thakur[3]
Information Technology Department
Prof. Ram Meghe Institute of Technology & Research,
Badnera-Amravati, India

Abstract: ***Wireless networks are improving in popularity to its peak today, as the user's demands for wireless connectivity regardless of their location. There is an increasing threat of attacks on the Mobile AdHoc Networks (MANET). However, its growth strongly relies on the availability of security services, among other factors. In the open, mutual MANET environment actually any node can maliciously or disrupts and deny communication of other hosts. However, energy constrained hosts, low channel bandwidth, node mobility, high channels error rates, channel variation and loss of packet are some of the drawbacks of MANETs. MANETs presents also security challenges. These networks are vulnerable to malicious attack, because any device within the vicinity of frequency range can get access to the MANET. There is a need for security system aware of these challenges. Thus, this work has vision to provide a secure MANET by changing the frequency range of data transmission. The security of data transmission is acquired without restrictive assumptions on the network nodes trust ability and network membership, and at the expense of improved multi-path transmission overhead only.***

Keywords: MANET, VANET, SMT, SRP.

I. INTRODUCTION

Worldwide business of smart phones, laptops, and PDAs has increased rapidly each year since their introduction. These mobile devices can be used to form MANETs. A MANET consists of arbitrary implemented communicational devices, such as cellular phones, Personal Digital Assistants (PDAs), laptop, etc. it is a multihop wireless network where all nodes collaboratively maintain the network connectivity. The mobile nodes are capable of connecting and communicating with each other using limited-bandwidth links. These types of networks are handy in any situation where temporary connectivity is needed and in areas with no required infrastructure, such as disaster site where existing infrastructure is damaged, or military operations where a tactical network is required. In a wireless ad hoc network where number of mobiles communicates by exchanging a variable amount of packets along routes set up by a routers routing algorithm, reliability may be defined as the ability to provide successful packet delivery rate. MANETs do not only provide dynamic infrastructure networks but also allow the flexibility to mobility of wireless devices. MANETs differentiate itself significantly from existing networks. Initially, the dynamic topology of the nodes in the network; Second, these networks are self configuring and do not require any centralized control or administration mechanism. These networks do not assume all the nodes to be in direct transmission vicinity of each other. Hence these networks require dedicated routing protocols that provide self-starting behavior. However energy constrained nodes, node mobility, low channel bandwidth, channel variability, and high channel error rates are some of the limitations of MANETs. Under such conditions, existing wired network protocols would crash or perform inefficiently.

Thus, MANETs require dedicated routing protocols. To secure the data transmission stages, 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 unknown, frequently changing networks in the presence of

adversaries that exhibit arbitrary malicious behavior. The goal of SMT is not to securely search for routes in the network the security of this stage should be achieved by protocols such as the secure routing protocol (SRP). The goal of SMT is to confirm secure data forwarding, after the establishment of routes between the source and the destination has secure data forwarding, In other words, SMT assumes that there is a protocol that searches for routes in the ad hoc network, although such searched routes may contain malicious nodes. An illustrative example of a single message transmission is shown in Fig. 1. The sender partitions the encoded message into four packets, so that any three out of the four packets are enough for successful reconstruction of the actual message. The four packets are routed over four disunited paths and two of them arrive intact at the receiver. The remaining two packets are loose by malicious nodes lying on the corresponding paths; for example, one packet is dropped, and one (dashed arrow) is modified.

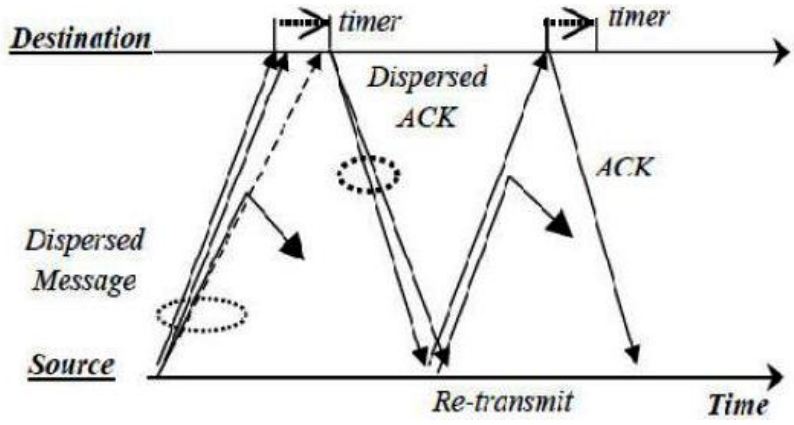

Figure 1: Simple example of the SMT protocol

The receiver take out the information from the first incoming validated packet and waits for later packets, while setting a receiving timer. When the fourth packet reaches, the cryptographic integrity check shows the data altering and the packet is rejected. At the exhaustion of the timer, the receiver creates an acknowledgement showing the two successfully received packets and feedback's the acknowledgment across the two active paths.

II. LITERATURE 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 them to have the shortest and high bandwidth available for the transmission such as in wormhole attack, and the attacker gets them in strong strategic place in the network. They make the use of their location that is 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 changing network i.e. frequently changing network, possibly in the presence of enemy. It combines four elements: end-to-end secure and robust feedback mechanism, dispersion of the transmitted data, simultaneous usage of different 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 contents than a protocol that don't give security to the data transmission. Moreover, SMT gives good result on alternative single path protocol, a secure data forwarding protocol we term

Secure Single Path (SSP) protocol. SMT creates up to 68% less routing overhead load than SSP, carries up to 22% more data packets and achieves end-to-end time delays that are up to 94% lower compared to SSP. Thus, SMT is better suited to support QoS for real-time communications in the ad hoc networking scenario. The safety of data transmission is achieved without restrictive assumptions on the network entities trust and network membership, without the use of intrusion detection schemes, and at the expense of modest multi-path transmission overhead only.

As for security solutions targeting MANET data transmission, the use of multiple routes residing in multi-hop topologies has been established in the early work of and then in. From a different Point of view, it has been proposed to detect misbehaving MANET nodes and report it to the rest of the network. All the network nodes keep a set of metrics showing 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 allow the misbehavior reports they exchange with their peers, searching to detect and isolate malicious nodes that do not forward data packets. Another method to detect an attacker staying on the utilized route has been proposed in [4]. Once the communication across the route sees a loss rate beyond a tolerable threshold, the source node starts a search along the route to determine where the failure occurred. To do so, an encrypted and authenticated dialogue is commenced 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.

III. SECURE MESSAGE TRANSMISSION

» ***Message Dispersion and Transmission***

The information dispersal scheme is taken from on Rabin's algorithm [3], which behaves in essence as an erasure code: it adds limited redundancy to the data to allow recovery from a number of errors. The message and the redundancy are divided into a number of parts, so that even a partial reception can lead to the successful reconstruction of the original message at the receiver. In principle, the encoding 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.

» ***Determination of the APS***

Underlying route discovery protocol, updates its network topology, and then determines the initial APS for communication with the specific destination. Otherwise, adversaries could reject communication by continuously providing wrong routing information. SMT is independent of the route discovery process – for example, it can function in conjunction with a reactive or a proactive protocol. However, the knowledge of the actual node 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 improve the reliability of the data transmission. For example, the path selection algorithm could incorporate subjective criteria, such as nodes to be directly included or excluded from the APS. Second, no discretion on route decisions is left to intermediate nodes, in order to improve the robustness of the protocol. This way, the communicating end nodes can directly correlate the failed or successful transmissions with the corresponding routes. As a result, nonfunctional and possibly unsecured routes are unambiguously detected at the initial node, so that newly determined routes can be entirely different from previously engaged and rejected 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 runs.

IV. APPROACH

» ***The security approach***

There are two main types of routing protocol in MANET (figure): proactive and reactive, Proactive protocols maintain recent lists of destinations and their routes by constantly distributing routing tables throughout the network. Reactive protocols find a route on demand i.e. only when needed by flooding the network with Route Request packets. Reactive protocols also known as on demand driven reactive protocols. The reason they are known as reactive protocols is, they do not start route discovery by themselves, until they are asked to do so, when a source node request to find a route. These protocols setup routes when demanded. When a node wants to communicate with other 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 requires some time to converge and then it will send 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].

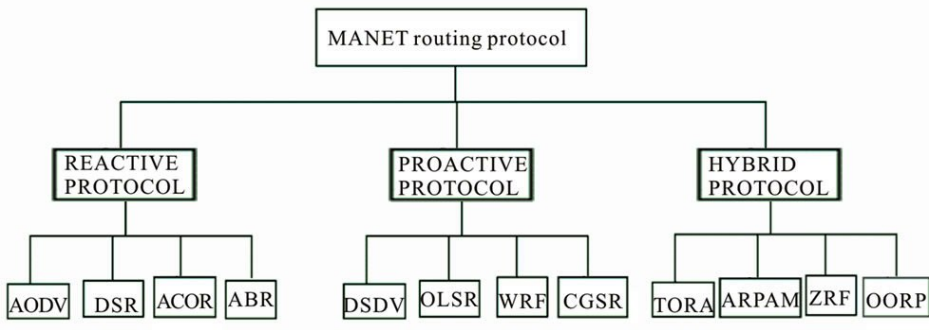

Figure2. Routing protocols classification

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

» **The mobility aware approach**

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

V. CONCLUSION

The SMT and SSP protocols for secure data communication in ad hoc networks. Both protocols are widely applicable, as they provide lightweight end-to-end security services, and function without knowledge of the trustworthiness of individual network nodes. They are highly efficient, highly reliable, less delay, and low-jitter communication even in highly unfavorable settings. SMT and SSP are flexible, 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 balance overhead for enhanced & efficient fault-tolerance and reliability, or balance 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.

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-outing-protocol- 00.txt, Dec. 2002.

AUTHOR(S) PROFILE

Rupesh M. Hushangabade, received the M.E degree in Information Technology from Prof.Ram Meghe institute of Technology & Research, Badnera-Amravati in 2013 and 2014, respectively. Currently working as an Assistant professor in Information Technology Department of Prof.Ram Meghe Institute of Technology & Research Badnera Amravati (Maharashtra).

Abhishek. A. Gulhane, received the M.E degree in Information Technology from Prof.Ram Meghe institute of Technology & Research, Badnera-Amravati in 2011 and 2012, respectively. Currently working as an Assistant professor in Information Technology Department of Prof.Ram Meghe Institute of Technology & Research Badnera Amravati (Maharashtra).

Smeet. D. Thakur, received the M.E degree in Information Technology from Prof.Ram Meghe institute of Technology & Research, Badnera-Amravati in 2013 and 2014, respectively. Currently working as an Assistant professor in Information Technology Department of Prof.Ram Meghe Institute of Technology & Research Badnera Amravati (Maharashtra).

