National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

NSF: A Novel Secure Framework for Protecting Route and Data in Mobile Ad-hoc Network

Lavanya N N[1], Pushpalatha R[2]
[1]M.tech in CS&E, VTU PG Centre, Mysuru, Karnataka, India
[2]Assistant professor, DOS in CS&E, VTU PG Centre, Mysuru, Karnataka, India

ABSTRACT

The adaptability and versatility of Mobile Ad hoc Networks (MANETs) have made them expanding prominently in a wide scope of utilization cases. To ensure the security, secure routing protocols have been designed to secure the routing paths and application information. In any case, these routing protocols just ensure route security or communication security, not both. Both secure routing and communication security routing protocols must be implemented to give full assurance to the network. To address these above issues, a secure framework, named NSF is proposed. The system is intended to permit existing system and routing protocols to play out their capacities, while giving node authentication, access control, and communication system security. This paper exhibits a security structure for MANETs. Comparison comes about looking at NSF with IPsec which is given to exhibit the proposed structures' appropriateness for communication security.
Keywords: access control, authentication, communication system security, mobile ad hoc networks.

I. INTRODUCTION

MANETs are dynamic, self-configuring, and infrastructure-less groups of mobile devices. They are usually created for a specific purpose. Each device within a MANET is known as a node and must take the role of a client and a router. Experts point out that the MANET, now a topic of commercial research, was originally used in military projects, including in tactical networks and Defense Advanced Research Projects Agency (DARPA) projects. Some use 4G networks and other wireless systems as examples of a potential topology for a MANET, while others refer to a vehicular ad-hoc network (VANET), where the free network nodes are installed in cars and other vehicles.

Those assessing the potential for MANET face various challenges, including signal protection and the reliability of mobile or otherwise dynamic nodes. There's also the issue of limited processing power, and even of providing an adequate power supply for the large number of devices typically included within a MANET. Still, the flexibility of a MANET makes this an interesting alternative to traditional networks structures. This paper proposes a novel security protocol, Novel Secure Framework for Protecting Route and Data in MANETs(NSF). The protocol is designed to address authentication of a node, network access control, and secure communication for MANETs using existing routing protocols. NSF combines routing and communication security at the network layer. This is in contrast to existing approaches, which provide only routing or communication security, requiring multiple protocols to protect the network. The Framework is designed to allow existing network and protocols to perform their function

whilst providing node authentication, access control, and communication security mechanisms.

The remainder of this paper is organized as follows: Section 2 analyses the problem in the context of previously published work. Section 3 introduces NSF, providing a technical discussion of the protocol. Section 4 outlines the characteristics chosen for modelling, and the results of simulating NSF compared against selected securerouting and data security protocols. Section 5 draws conclusions from the research findings.

II. RELATED WORK AND PROBLEM ANALYSIS

Ad hoc On-demand Distance Vector routing protocol: MANETs depend on intermediate the way in which packets are steered to their goals, MANET routing protocols rather make utilization of routing tables on each node in the system, containing either full or fractional topology data. Reactive protocols, for example, Ad hoc On-request Distance Vector (AODV) arrange routes when messages should be sent, surveying close-by nodes trying to locate the nearest route to the destination node.

Optimized link state routing protocol: In this paper we propose and discuss an optimized link state routing protocol, named OLSR, for mobile wireless networks. The protocol is based on the link state algorithm and it is proactive (or table driven) in nature. It employs periodic exchange of messages to maintain topology information of the network at each node. OLSR is an optimization over a pure link state protocol as it compacts the size of information sent in the messages, and furthermore, reduces the number of retransmissions to flood these messages in an entire network. For this purpose

MANET Routing Security: To handle the issues that accepted authenticity can bring about, secure MANET directing conventions have been proposed. Secure Ad hoc On-request Distance Vector (SAODV) and Secure Optimized Link State Routing (SOLSR) are secure usage of AODV and OLSR separately. SAODV secures the directing system by incorporating irregular numbers in Route Request bundles (RREQs). On the off chance that a steering bundle arrives that re-utilizes an old parcel number, that bundle is invalid. Hubs watched sending re played bundles might be hailed as malevolent. SAODV requires that no less than two Secure RREQs (SRREQs) touch base at the goal hub by various courses with indistinguishable irregular numbers to distinguish the source hub. Security Communication: Securing courses is just a single part of a full security arrangement. X.805 highlights numerous security dangers including personality, information control, debasement and robbery. There are three prerequisites to securing correspondence; confirmation, classification and respectability. X.509 sets the standard for endorsement based ways to deal with security. Authentications give a suite of information that can be utilized to speak to the character of a given hub, and its association with a confided in specialist.

Summary: NSF, the convention proposed in this paper, addresses the issue of bound together MANET correspondence security. It executes a Virtual Closed Network design to ensure both system and application information. This is conversely with the methodologies proposed in past work, which concentrate on ensuring particular correspondence based administrations.

III. THE NSF FRAMEWORK

The protocol, NSF is designed to work in network layer. The packets from transport layer is forwarded to data link layer through NSF. The main functions of network layer are to identify the nodes and create routing tables. NSF is designed to provide authentication in the network layer end to end i.e., source to destination nodes.

A. NSF Framework Overview

The routing table maintains the route information, source id, destination ID, etc. The routing header extracts all the routing table information. NSF is also designed to provide authentication in the network layer point to point i.e., intermediate nodes and end to end i.e., between source and destination. For this purpose, a security table is maintained which contains the key information Once the authentication is done the message is forwarded to the data link layer. It is designed to provide a fully secured communication framework for MANET's, without requiring modification of the routing protocol. Figure 1 shows the flow of data from transport, through the network layer (including NSF) to data link layer. MANET routing protocols require broadcast capabilities.

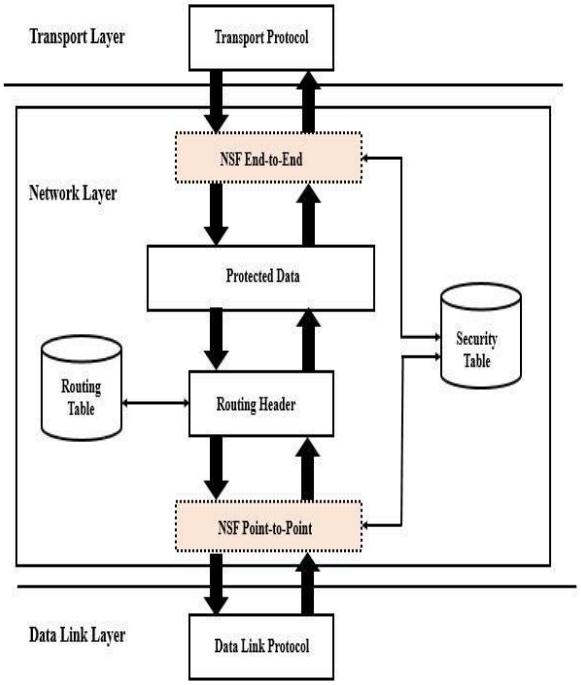

Figure 1. Diagram illustrating the NSF confidentiality, integrity and authentication services for data packets.

B. MODULES

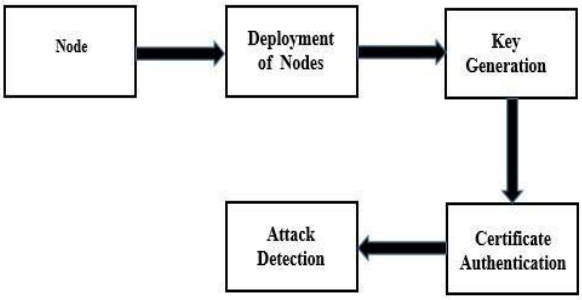

Figure 2

Deployment of Nodes

The nodes are deployed based on a particular topology and specifying x axis and y axis values. Also node id is specified. Node id of the nodes changes as and when the application restarts.

Key Generation

To Provide Secure communication NSF relies on the dynamic generation of keys.

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. The key generated will be stored in a security table maintained at each node.

Secure Keys

Secure key(SKe) are used to secure source and destination with one SKe key generated per node. Secure Key(SKp) are shared between two nodes used to authenticate traffic as it moves along the network.

Symmetric Broadcast Key

A Symmetric broadcast key will be generated at the initialization of the network when first node to be contacted about joining to the network.

Symmetric broadcast key has two derived forms Symmetric broadcast end-to-end (SKbe) key and Symmetric point-to-point key(SKbp), In end-to-end broadcast communication SKbe provides confidentiality. In point-to-point broadcast

communication packet integrity by generating tags using hash function.

Certificate Authentication

NSF uses a certificate based approach to authenticate new node and allow them to become member of the network if they appropriate credentials. Once authenticated with the network a node will begin to form secure links, by associating itself with other member nodes on-demand.

NSF node must exchange a key share with other nodes receiving this in response and performing key exchange to generate appropriate keys for end-to-end and point-to-point cryptographic functions. The nodes are verified for validity. If the nodes are valid then the packet will be transmitted. If the nodes are invalid, then no packets are transmitted. NSF will only begin routing once node have been authenticated with the network (i.e,. receiving broadcast keys in the process).

Attack Detection

The certificate authority is going to verify the RREP AND RREQ packets. If the sequence number are not matching, then attack is detected otherwise no attack is detected.

IV. SUMMARY

MANET routing protocols require broadcast capabilities. Both OLSR and AODV require broadcast communication for routes discovery. NSF provides broadcast communication security services to allow it to service the specific needs of MANET routing protocols. NSF addresses the eight security dimensions detailed by X.805 by providing a closed-MANET, with end-to-end and point-to-point security features. The eight security dimensions are addressed as follows.

- **Access control** is provided by NSF network joining method.
- **Authentication** is provided by certificates.
- **Non-repudiation** is provided by timestamps.
- **Confidentiality** is provided end-to-end by payload encryption using AEAD.
- **Communication** security is maintained by encrypting and performing source authentication end-to-end, and checking authenticity and integrity at each hop.
- **Availability** is maintained using each nodes security table, which stores valid authentication credentials.
- **Privacy** is provided by end-to-end encryption, with keys that are specific to the link between two nodes or a node and the network.

V. CONCLUSION

NSF is a security framework that protects the network and communication in MANETs. The primary focus is to secure access to a virtually closed network (VCN) that allows expedient, reliable communication with confidentiality, integrity and authenticity services. NSF addresses each of the eight security measurements plot in x.805. In this manner, NSF can be said to actualize a full suite of security administrations for self-sufficient simulation has been attempted and the outcomes are accounted for and investigated to decide the relative cost of security. NSF has been shown to provide lower-cost security than SAODV for their routing protocols by stablishing a secure, closed network; one can assume a certain level of trust within that network. This reduces the need for costly secure routing behaviors designed to mitigate the effects of an untrusted environment (and untrusted nodes) on the routing process. By preventing the entry of potentially untrustworthy nodes to the network, and thus the routing process, a MANET may be protected from subversion of its routing services at a lower cost, as malicious nodes are barred from the process entirely.

VI. FUTURE WORK

Future work includes the implementation of NSF on a simple mobile node platform to allow experimental observation and profiling of its performance. The

proposal of network bridging solutions capable of providing NSF services between two closed networks over an insecure intermediate network, and investigating the effects of variable network topology on NSF to better understand the role of the credential referral mechanism on overhead mitigation in networks.

VII. REFERENCES

[1] P. S. Kiran, "Protocol architecture for mobile ad hoc networks," inProc. IEEE Int. Ad. Comput. Conf., 2009, pp. 2112–2117.

[2] Chandra, "Ontology for manet security threats," in Proc. 2nd Nat. Conf. Netw. Eng., 2005, pp. 171–117.

[3] K. Rai, R. R. Tewari, and S. K. Upadhyay,

[4] "Different types of attacks on integrated manetinternet communication," Int. J.Comput. Sci. Secur., vol. 4, no. 3, pp. 265–274, 2010.

[5] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, "A cluster- based approach to consensus based distributed task allocation," in Proc. 22nd Euromicro Int. Conf. Parallel, Distrib. Netw.-Based Process., 2014, pp. 428–431.

[6] I. D. Chakeres and E. M. Belding-Royer, "Aodv routing protocol implementation design," in Proc. 24th Int. Conf. Distrib. Comput. Syst. Workshops, 2004, pp. 698– 703.[6] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," RFC 3626, Oct. 2003, Doi: 10.17487/RFC3626.

[7] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. Temple, "Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles," in Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops, 2007, vol. 2, pp. 249–256.

[8] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uav swarming applications," in Proc. 8th Int. Symp. Wireless Commun. Syst., 2011, pp. 317–321.

[9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Commun., vol. 11, no. 1, pp. 38–47, Feb. 2004.

[10] [10] N. Garg and R. Mahapatra, "Manet security issues," Int. J. Comput.Sci. Netw. Secur., vol. 9, no. 8, pp. 241–246, 2009.