Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

ASF: An Authenticated Security Framework Protecting Routes and Data in MANETs

Pavan Guptha T H, S Deekshitha, Samarth B, Sushma C

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 ASF 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 ASF with IPsec which is given to exhibit the proposed structures' appropriateness for communication security.

Index Terms—access control, authentication, communication system security, mobile ad hoc networks

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. Communication across the network is achieved by forwarding packets to a destination node; when a direct source-destination link is unavailable intermediate nodes are used as routers. MANET communication is commonly wireless. Wireless communication can be trivially intercepted by any node in range of the transmitter. This can leave MANETs open to a range of attacks, such as the Sybil attack and route manipulation attacks that can compromise the integrity of the network. A MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)--herein simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. In the latter operational mode, it is typically envisioned to operate as a "stub" network connecting to a fixed internet work.

Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network. MANET nodes are equipped with wireless transmitters and receivers using antennas which may be Omni directional (broadcast), highly- directional (point-to-point), possibly steer able, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

MANET Characteristics:

1) Distributed operation: There is no background network for the central control of the network operations, the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

2) Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

3) Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.

4) Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.

5) Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

6) Shared Physical Medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

MANET Routing Protocols:

Ad-Hoc network routing protocols are commonly divided into three main classes:

1) Proactive Protocols: Proactive, or table-driven routing protocols. In proactive routing, each node has to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. Example of such schemes are 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 allow nodes to quickly determine which nodes are present or reachable in the network.

2) Reactive Protocols: Reactive routing is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wants 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 occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV) [11] and Dynamic Source Routing (DSR).

3) Hybrid Protocols: They introduce a hybrid model that combines reactive and proactive routing protocols. The Zone Routing Protocol (ZRP) is a hybrid routing protocol that divides the network into zones. ZRP provides a hierarchical architecture where each node has to maintain additional topological information requiring extra memory.

RELATED WORK

Dareen Smith et al., [1] presented a novel extension to the Consensus-Based Bundle Algorithm (CBBA), which we have named Cluster-Formed Consensus-Based Bundle Algorithm (CFCBBA). CF-CBBA is designed to reduce the amount of communication required to complete a distributed task allocation process, by partitioning the problem and processing it in parallel clusters. CF-CBBA has been shown, in comparison with baseline CBBA, to require less communication when allocating tasks. Three key aspects of task allocation have been investigated; (a) the time taken to allocate tasks, (b) the amount of communication necessary to satisfy the requirements of distributed task allocation algorithms such as CBBA, and (c) the efficiency with which a collection of tasks (a mission) is completed by a group of robots (a collective).

Shushan Zhao et al., [7] found out a Key Management (KM) and Secure Routing (SR) which are two most important issues for Mobile Ad-hoc Networks (MANETs), but previous solutions tend to consider them separately. This leads to KM-SR interdependency cycle problem. Here we propose an

integrated KM-SR scheme that addresses KM-SR interdependency cycle problem. By using identity based cryptography (IBC), this scheme provides security features including confidentiality, integrity, authentication, freshness, and non-repudiation.

Nishu Garg et al., [4] In order to avoid all the performance loss, they developed a technique to periodically discover shortcuts to the active routes that can be used with any destination vector routing protocol. It also shows how the same mechanism can be used as a bidirectional route recovery mechanism. Consider the problem of incorporating security mechanisms into routing protocols for ad hoc networks. Canned security solutions like IPSec are not applicable. We look at AODV in detail and develop a security mechanism to protect its routing information. The key contributing factor to this problem is an inability to distinguish legitimate nodes from malicious nodes.

Andrew R et al., [6] proposed the X.805 Security Architecture which defines the framework for the architecture and dimensions in achieving end-to-end security of distributed applications. The general principles and definitions apply to all applications, even though details such as threats and vulnerabilities and the measures to counter or prevent them vary based on the needs of the application. How each standard fits together in the end-to-end security picture emanates from X.80S. lTV-T Recommendation X.80S. Describes the wireless end-to-end security in seven classification & convenient identification of security threats.

Hao Yang et al., [2] focused on the fundamental security problem of protecting the multihop network connectivity between mobile nodes in a MANET. We identify the security issues related to this problem, discuss the challenges to security design, and review the state-of-the-art security proposals that protect the MANET link- and network-layer operations of delivering packets over the multihop wireless channel. The complete security solution should span both layers, and encompass all three security components of prevention, detection, and reaction.

PROBLEM ANALYSIS

MANET Security: MANETs depend on intermediate nodes to route messages between legitimate nodes. Lacking framework to administrate 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.

Security Threats: The ITU-T Recommendations through X.805, characterizes remote end to-end security in seven characterizations, which are called measurements. This arrangement of characterization takes into consideration clear and advantageous recognizable proof of security dangers in a systems and potential answers for those issues. The following are the accompanying security measurements that are recognized.

- Access control is required to ensure that malicious nodes are kept out of the network.
- Authentication confirms the identity of communicating nodes.
- Non-repudiation prevents nodes from broadcasting false information about previous transmissions, mitigating replay and related attacks.
- Confidentiality prevents unauthorized nodes from deriving meaning from captured packet payloads.
- Communication security ensures that information only flows between source and destination without being diverted or intercepted.
- Integrity checking allows nodes to ensure packets received are in the same form they were sent, without modification or corruption.
- Availability ensures that network assets are accessible. Periodic checking of node status or reports from a node to its neighbors are a common means of checking the availability of a resource.
- Privacy prevents outside observers from deriving valuable information through passive observation.

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: ASF, 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.

THE ASF FRAMEWORK

The protocol, ASF is designed to work in network layer. The packets from transport layer is forwarded to network layer. The main functions of network layer are to identify the nodes and create routing tables. ASF is designed to provide authentication in the network layer end to end i.e., source to destination nodes. Confidentiality and integrity of the nodes is preserved. The routing table maintains the route information, source id, destination ID, etc. The routing header extracts the routing table information. ASF is also designed to provide authentication in the network layer point to point i.e., intermediate nodes. 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.

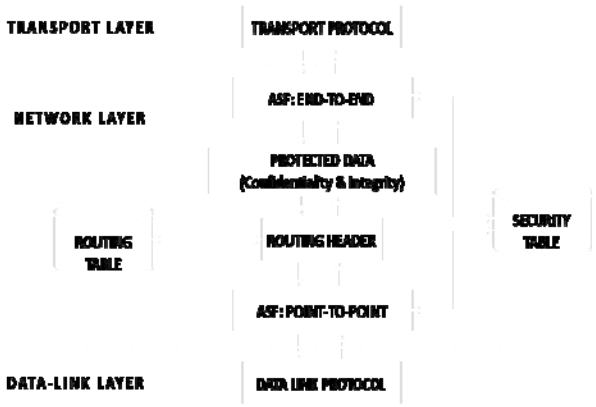

Fig. 1: Diagram illustrating the ASF confidentiality, integrity and authentication services for data packets

MODULES

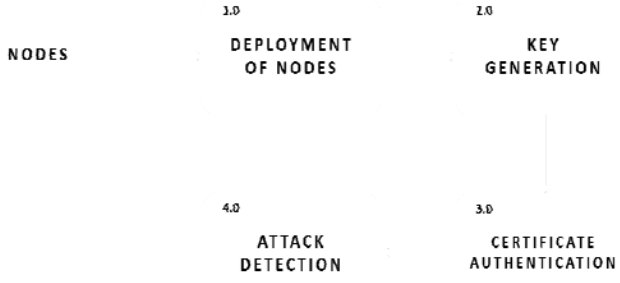

Fig 2: Modules of the ASF Framework

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

The deployed nodes are subjected to Elliptic Curve Cryptography. 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 file.

CERTIFICATE AUTHENTICATION

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.

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.

ELEPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra elliptic curve factorization.

The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005.

For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation $y^2=x^3+ax+b$ along with a distinguished point at infinity, denoted ∞. (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.)

Unlike most other DLP systems (where it is possible to use the same procedure for squaring and multiplication), the EC addition is significantly different for doubling (P = Q) and general addition (P ≠ Q) depending on the coordinate system used. Consequently, it is important to counteract side channel attacks (e.g., timing or simple/differential power analysis attacks) using, for example, fixed pattern window (a.k.a. comb) methods (note that this does not increase computation time). Alternatively one can use an Edwards curve; this is a special family of elliptic curves for which doubling and addition can be done with the same operation. Another concern for ECC-systems is the danger of fault attacks, especially when running on smart cards.

RESULTS

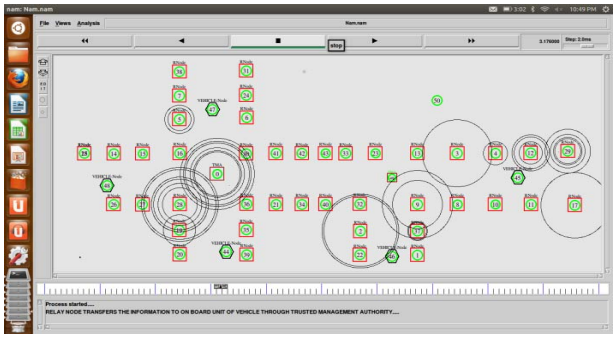

Fig 3: Ad-hoc Network of 50 Nodes Deployment

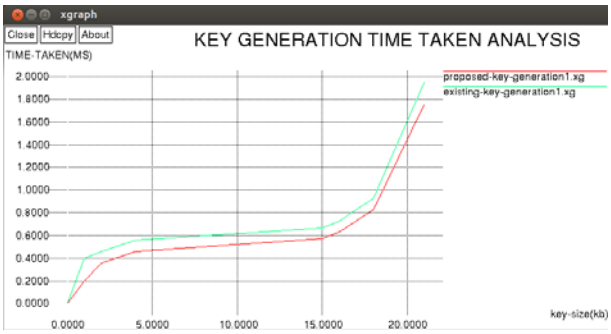

Fig. 4: Key Generation Time Taken Analysis for each Node

The simulation studies involve the deterministic traffic network topology with 50 nodes as shown in Fig 3. The proposed energy efficient algorithm is implemented with NS2. We transmitted same size of data packets through source node 1 to destination node 50. Proposed framework is compared between two metrics, Total Transmission Energy and Maximum Number of Hops on the basis of total number of packets transmitted, network lifetime and energy consumed by each node. We considered the simulation time as a network lifetime and it is a time when no route is available to transmit the packet. Simulation time is calculated through the CPUTIME function of NS2. Results shows that the throughput, delay time taken for transmission and key generation time taken analysis through the network.

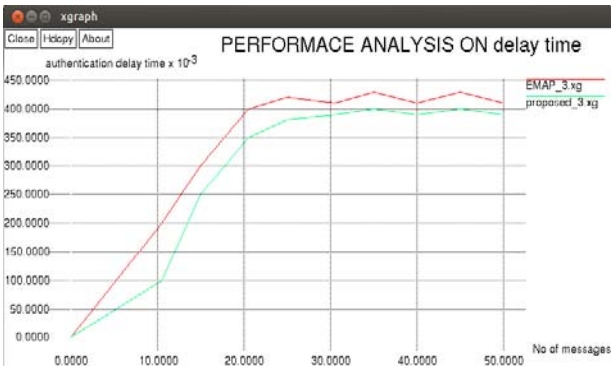

Fig. 5: Performance Analysis on delay time

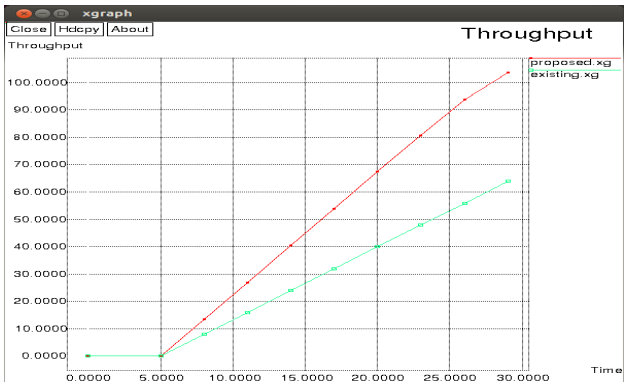

Fig 6: Throughput of the system

The network topology is showed in Fig. 3 which shows the traffic management scenario. Here the nodes are deployed with relay nodes monitoring the traffic. It senses the vehicular movement and transmits the information to the TMA. Fig. 4 shows the Key Generation Time Taken for each Node. In the graph the existing system consumes more time to generate the key for detecting unauthorized nodes whereas the proposed takes considerably less time. Fig. 5 shows the performance analysis of the system in terms of delay time taken for the data transmission. Initially the delay increases gradually for less number of messages and further remains stable at significant point of time with increase in the message count. Fig. 6 shows the throughput of the system. Results show that the proposed system is better than the existing systems considering the suitable analysis for delivering the packets successfully.

CONCLUSION

ASF 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. ASF addresses each of the eight security measurements plot in x.805. In this manner, ASF 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. ASF has been shown to provide lower-cost security than SAODV for their routing protocols by establishing 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.

FUTURE WORK

Future work includes the implementation of ASF on a simple mobile node platform to allow experimental observation and profiling of its performance. The proposal of network bridging solutions capable of providing ASF services between two closed networks over an insecure intermediate network, and investigating the effects of variable network topology on ASF to better understand the role of the credential referral mechanism on overhead mitigation in networks.

References

1] Darren Hurley-Smith, Jodie Wetherall and Andrew Adekunle “SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad-hoc Networks”, IEEE Transactions on Mobile Computing, pp. 1-15, 2016.

[2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in Mobile Ad-hoc Networks: Challenges and Solutions,” Wireless Communications, IEEE, vol. 11, no. 1, pp. 38-47, 2004.

[3] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, “A Cluster-based Approach to Consensus based Distributed Task Allocation,” in Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euromicro International Conference on. IEEE, 2014, pp. 428–431.

[4] N. Garg and R. Mahapatra, “MANET Security Issues,” IJCSNS, vol. 9, no. 8, p. 241, 2009.

[5] W. Ivancic, D. Stewart, D. Sullivan, and P. Finch, “An Evaluation of Protocols for UAV Science Applications,” 2011.

[6] A. R. McGee, U. Chandrashekhar, and S. H. Richman, "Using ITU-T x. 805 for Comprehensive Network Security Assessment and Planning", pp. 273–278, 2004.

[7] S. Zhao, R. Kent, and A. Aggarwal, "A key management and secure routing integrated framework for mobile ad-hoc networks," Ad Hoc Networks, vol. 11, no. 3, pp. 1046–1061, 2013.