The Research of Trusted Security Architecture of MANET Node Based on OPNET

Zhen Zhang

Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China

Keywords: OPNET, MANET, security architecture, trusted.

Abstract. MANET has been widely used in some special application scenarios, but because of its own characteristics lead to less secure and easily be attacked, resulting in significant losses. In response to this situation, this paper proposes a new trusted security architecture of MANET nodes based OPNET. Borrowing the concept of trusted computing, to provide joint security in the MAC layer and network layer of multi-level, better than the traditional single-level security. According to the simulation results, we found little effect on the performance of the network, which can effectively improve the security of MANET.

1. Introduction

MANET (mobile ad-hoc network) that is composed of a group of mobile terminals with wireless transceiver consisting of non-base station, multi-hop, temporary network system, widely used in some special environment that is military battlefield, Emergency rescue or disaster relief. It is no centre, peering, openness, limited resources and other characteristics, vulnerable to be attacked, such as black holes, wormholes attacks, replay attacks, eavesdropping, sleeping deprivation and so on, so its safety has been the focus of attention. MANET security measures existing currently almost aim at a certain level that is only for MAC, or only for the route, there is rarely a security architecture which can provide multi-level protection for MANET network.

2. The design of security architecture

2.1 The overall design of security architecture

Traditional MANET security almost aim at the single level of OSI layers, with certain limitations, is relatively easy for malicious attackers. This paper proposes a multi-level joint cross-layer security architecture, according to the MAC layer and network layer, adding the support of TPM module [1] and the concept of cross-layer, making a great robust security system. Architecture as shown in Fig.1.

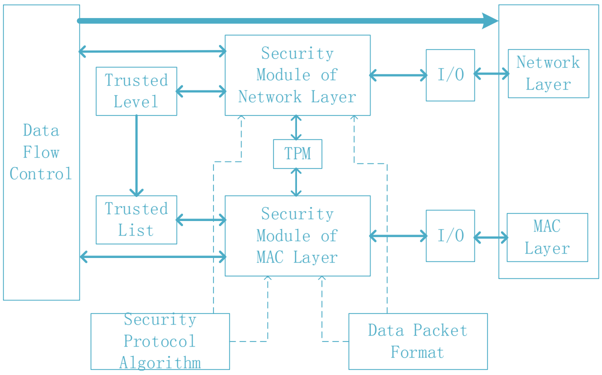


Fig.1: Security architecture

In order to achieve the purpose of standardization platform architecture, security protocols algorithm replaceable and standardized packet format for security protocols are needed for network layer and mac layer security module to support. The two modules maintain respectively the trusted level and the trusted list. TPM provide support for identity authentication and integrity measurement to security modules through its endorsement key EK, authentication key AIK, other keys and certificates. Through their respective I / O interface, the modules connect with the network layer or access layer, verify the nodes that packets come from. According to the results authenticated, the security module labeled its trusted level and whether it was in the trusted list, trusted level of the network layer would feedback to the trusted list of security management module of mac layer, reaching the purpose of dual certification to nodes and more and more trusted. Data flow control shall be in accordance with the certified results of the mac layer or network layer security modules, in order to continue to submit the package to the upper or lower, or will be discarded.

2.2 Functional design of each module

2.2.1 Functional design of mac layer security module

In order to achieve the goal of trusted mac layer, the concept of trusted network connection (TNC) [2] has been introduced to this layer with the user and platform identity authentication and integrity measurement.

Mac layer security module is divided into three major functional areas: 1) the list maintenance area, the mac layer in the maintenance of a trusted list and a list of nodes that has proposed an access request; 2) the security core functional areas, TNC is the core module of this area; 3) data processing area, under the role of the security core functional areas, discarded or forwarded packets in accordance with its instructions.

Fig.2 is a schematic diagram of the mac layer security module function. After receiving the package from lower, it should be checked whether the node that the packet comes from is in the trusted list. If it is a trusted node, the data will be submitted directly to the data processing area and forwarded process; if not, trusted verification will be needed. First the module judges whether the access request has been submitted, discards the packet directly if it is, if not, enters into the core functional areas and carry out the process TNC. According to the results of the TNC process, if the module judged to be trusted, add the node that packets come from to the trusted list and forwards the packet, otherwise discarded.

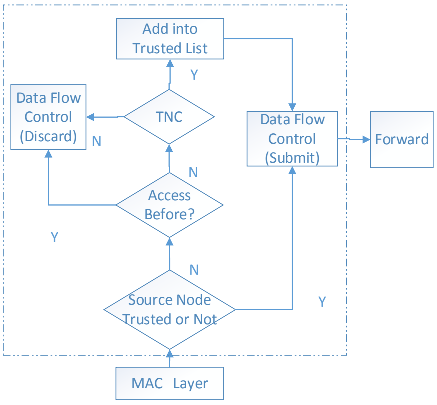
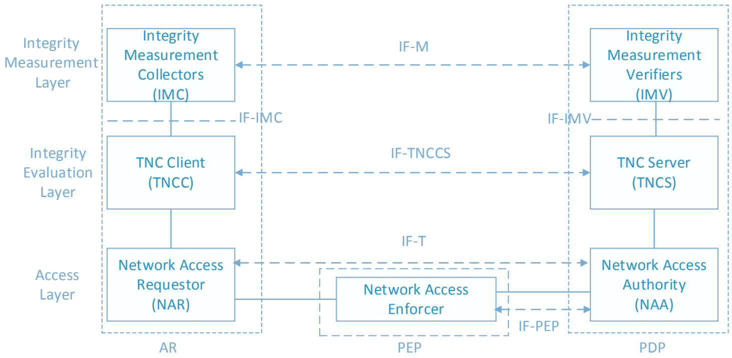

Add into Trusted List
Y
Data Flow Control (Discard)
TNC
N
Data Flow Control (Submit)
Forward
N
Access Before?
Y
N
Source Node Trusted or Not
Y
MAC Layer

Fig.2: The flow of security module of mac layer

2.2.2 The Workflow of mac layer main security module

Mac layer security module has borrowed the concept of TNC. Identity authenticate and integrity measure the access request of other nodes and TPM module involve in the correlation calculation and storage. Node's user and platform identity authentication, platform integrity measurement execute in sequence. Before accomplishing all these, there is a terminated connection if one step not be passed. The TNC process as shown in Fig.3.



Integrity Measurement Layer
Integrity Evaluation Layer
Access Layer
Integrity Measurement Collectors (IMC)
TNC Client (TNCC)
Network Access Requestor (NAR)
IF-IMC
IF-M
IF-TNCCS
IF-T
IF-IMV
IF-PEP
Network Access Enforcer
Integrity Measurement Verifiers (IMV)
TNC Server (TNCS)
Network Access Authority (NAA)
AR
PEP
PDP

Fig.3: The TNC process

Step 1: Before node's user and platform identity authentication as well as platform integrity measurement, TNCC and TNCS needs to be initialized to IMC and IMV respectively.

Step 2: When an authentication request occurs, NAR sends a request to PEP. After the PEP receiving the request, PEP sends an authentication decision request to NAA. User authentication occurs between NAA and AR, platform authentication and integrity checking occurs between AR and TNCS.

Step 3: If the user authentication is completed successfully, the NAA notices TNCS platform authentication request arrives, TNCS and TNCC platform for verification.

Step 4: If the platform between TNCC and TNCS verification has been completed successfully. TNCS notices IMV new request occur and needed, need for integrity verification. Meanwhile TNCC notices IMC new request occur and needed, need preparing the relevant information integrity.

Step 5: TNCC and TNCS exchange kinds of information related to integrity verification. TNCS sends each message from IMC to the IMV. IMV analyses the integrity information collected by IMC. And then IMV will send the results to TNCS. This information will be forwarded by NAR, PEP and NAA until the integrity status of AR meet the requirements of TNCS

Step 6: After integrity checking being completed by TNCS, and it notices the NAA that notice the PEP to perform decision of the PDP to complete the trusted connection.

2.2.3 Functional Design of Network Layer Security Module

Network layer security module functions Similar to the mac layer, divide into four main functional areas. First, the authentication information encapsulation area. In the routing maintenance control packets encapsulate authentication information for periodic authentication provides relevant packet. Second, trusted level recording area. Different to mac layer, trusted level list record a variety of properties (≥3 kinds) rather than trusted list that record only two properties about yes or no, and it can be extended to a more detailed list of multi-level in order to accommodate the needs of different security environment. There are four trusted levels designed here (Trusted, Medium, Black, Unknown, of course you can design more detailed levels). Third, signature verification functional area. This area is the core of network layer security module. Fourth, data processing area. This area feature is same to mac layer security module for packets discarded or forwarding.

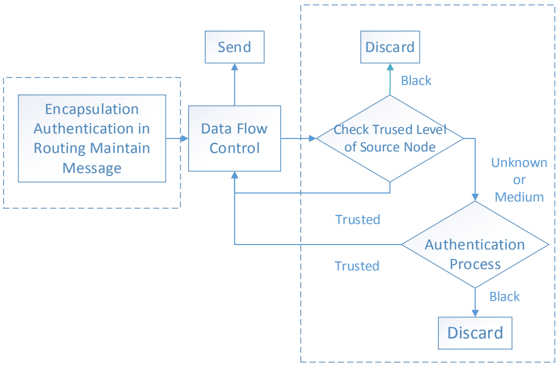


Fig.4: The process of network layer security module

The Fig.4 is a functional diagram of the network layer security module. During to network nodes working online, the routing protocol has been maintained routing table all the time. It sends a HELLO packet every time period. It is very convenient for encapsulating signature or authentication information in such routing maintenance packets for periodic verification. As the network layer security authentication starting, first encapsulate signature authentication information, and deliver it to data flow control module for sending. As the receiving packets from another node, check the trusted level of source node. If for trusted, then forward to upper. If for Black, then discarded. If for other Level indicators, then conduct the signature verification process in order to verify trusted or not. It fails, mark as Black and discarded.

2.2.4 The Workflow of Network Layer Main Security Module

Network layer security module is mainly realized by remote attestation, it is a process that the challenger proved the trusted itself to responder. The responder with a series of authentication using different AIK that is different from mac layer based on evidence provided by the challenger determines the credibility of the challenger.

Now more commonly used methods of remote attestation are property-based (PBA [3], SBCFI [4], etc.) based information flow (BIND [5], Dr@ft [6], etc.), based on the behaviour (Tamleek [7], etc.) as well as direct anonymous authentication (DAA) protocol [8] and its variants. At present, remote attestation property-based is a method most suitable for resolving the platform integrity issue, and select a solution to identity authentication, such as DAA protocol. The authentication process between challenger and responder as follows:

Step 1: Before joining the network, each node is first initialized. The both sides of nodes obtain a certificate from the issuer to generate direct anonymous authentication signature key in the offline case.

Step 2: As the network layer to be trusted authentication, hello message is sent $node_j$ send to $node_i$ encapsulate the DAA signature of their own and the HashSign of hello message. Inside, HashSign is a lightweight signature algorithm binding to the node itself in order to prove the source of the signature from this node.

Step 3: After the $node_i$ receives hello message of $node_j$, to verify the DAA and HashSign signature from the package. It is successful, a VerifyRequest message encapsulates a random number n_i, a shared key k_i between $node_i$ and $node_j$, a DAA signature to $node_i$ and the HashSign signature to VerifyRequest messages is sent, and requires $node_j$ to reply a signature of property-based remote attestation aimed to n_i.

Step 4: After $node_j$ receives VerifyRequest message from $node_i$, verify DAA and HashSign signature. If successful, send VerifyReply message. Which encapsulates the property-based remote attestation aimed to random number n_i sent by $node_i$, a challenge random number n_j, shared key k_j between $node_i$ and $node_j$, and the HashSign signature of VerifyReply messages. And then require $node_i$ to reply the property-based remote attestation aimed to n_j.

Step 5: After the $node_i$ receives VerifyReply message from $node_j$, verify HashSign signature and property-based remote attestation signature of n_j . If successful, the shared key n_{ij} composed of n_i and n_j, and use this key to encrypt VerifyOK message, which encapsulates the property-based remote attestation signature of n_j. And then send it to $node_j$.

Step 6: After $node_j$ receives VerifyOK message from $node_i$, verify property- based remote attestation signature. If successful, the two sides are mutual trusted.

Step 7: If any part of the authentication fails in the above process, the whole process is terminated and the parties are not mutual trusted.

2.2.5 Cross-Layer Interaction

Network layer and mac layer need to cross-layer interact with the results of the whole authentication, integrate authentication result, achieve the effect of 1+1>2. At the end of the authentication process, regardless of it is Trusted, Medium or Black, network layer will send a remote interrupt to access layer that notify the authentication results of network layer to the access layer. Since the node through the access layer trusted connection firstly, it can continue to submit data upper. So if the network layer authentication decision is trusted or medium for external node, the trusted list of the node retained. If it is Black, this node in trusted list should be changed from Trusted to Black by mac layer, and the access is forbidden, in order to making further enhance network security.

2.3 Packet format

2.3.1 Packet format of mac layer security module

At the Mac layer module adding the TNC control package, further encapsulated based on mac layer packets. The packet format is as follows:

Mac message	TNC_flag	Signature data	Shared key

Mac_message: MAC layer standard message.

TNC_flag: Mark the node at which stage of the TNC process currently.

Signature data: a variety of authentication signature information of TNC stage and used to be verified.

Shared key: $node_i$ and $node_j$ in the process of mutual authentication, the module encapsulate k_i, k_j and a combination of the shared key k_{ij} in each packet.

2.3.2 Packet format of network layer security module

In the process model of various types of routing protocols at OPNET MODELER environment, we modify the handshake process of HELLO message issued when the route maintenance, encapsulate a series of signature data in them. Its packet format is as follows:

Packet type	Trusted level	Shared key	Signature data	Random number

Packet type: Includes initial HELLO package, or relevant data packet types of custom authentication process.

Trusted level: The trusted level is defined the number of levels (the number of levels ≥3) based on specific practical needs, containing at least 3 kinds: TRUSTED, UNKNOWN and BLACK. Also depending on the circumstances, fine-grained division of trusted levels, so that better security controls.

Shared key: That is, $node_i$ and $node_j$ in the process of mutual authentication encapsulate k_i, k_j and a combination of the shared key k_{ij} in each packet.

Signature data: Here is HashSign signature, remote anonymous authentication signature, property-based remote attestation signature, or other remote attestation signature.

Random number: When the authentication request or response is sent, the challenge random number is encapsulated or used in the process of remote attestation.

3. The Simulation Results and Analysis

Table.1: Simulation parameters

Scene area ：2 x 2 km	Nodes numbers：8
The communication distance between nodes ：0.4-0.8km	Simulation time：600s
Moving rate ：1-2m/s	Moving time ：10-420s
Moving mode：random waypoint	Transmission rate ：1Mbps
Mac layer protocol：802.11 DCF	MANET route protocol：AODV

The security architecture using OPNET MODELER 14.5 simulation platform, simulation environment make the settings in Table.1:

3.1 Performance Evaluation of Security Architecture

In order to evaluate the performance of the security architecture, we need to compare throughput, load and end to end delay with MANET ordinary nodes. According to the present simulation parameters the following three pieces of comparison chart are contained in Fig.6. After adding the security architecture we found throughput, load higher than ordinary nodes. Because of authentication and integrity checking interact packet sent numbers and large packet sizes than the ordinary nodes, so throughput is little large. After adding security architecture, load of nodes is much higher than normal nodes at the beginning stages of security authentication and moving, and then begin to decrease. Until stopping moving at seven minutes, data transceiver is to stabilize, and throughput is just a little higher than moving. Because of stopping, so after seven minutes the load has a small rise of ordinary nodes, and basically stabilized of security node. We can find clearly the overall status of security architecture from end-to-end delay. In the initial stage of connection being established, various security authentication is needed.So the end-to-end delay will be relatively large, but this time is short. In about ten seconds, end-to-end delay decreased rapidly, eventually close to ordinary node. From the three simulation results, the security architecture has less impact on network performance, and can effectively improve network security.

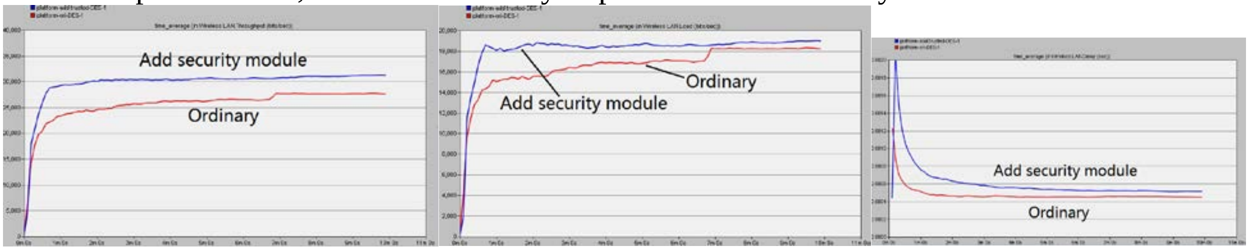


Fig.6: Throughput (upper left), load (upper right), end-to-end delay (lower)

3.2 Network Performance under Black Hole Attack

Black hole attack is a common form of attack in the network, claiming to neighbour node that it has the optimal routing and the minimum number of hops to the destination node in the network. When attracting packets through this node, route maintenance and data packets are discarded, so that normal business is affected worse in network. We change one node into black hole attack node of simulation environment for simulate betrayed. The Fig.7 (left) is displayed that throughput of ordinary MANET network suffers severe decline under black hole attack, it seriously affect the normal use of the network. While the Fig.7 (right) is the result of adding security architecture under black hole attack in MANET, throughput has improved significantly compared to ordinary network. Due to a node that lack of the throughput as a betrayer, and the actual throughput decline is not obvious. Visible, security architecture proposed in this paper to enhance the security of MANET network is quite effective.

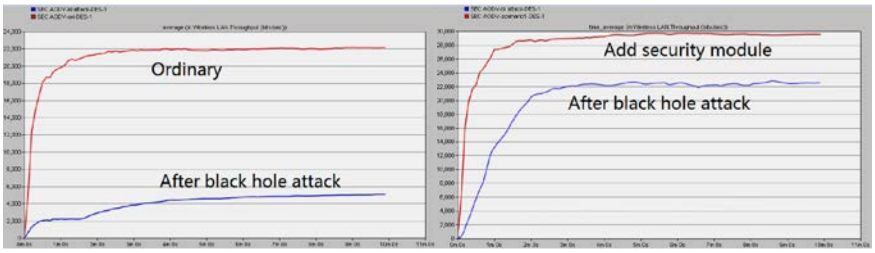


Fig.7: Throughput of ordinary (left), add security module (right)
under black hole attack

4. Conclusion

From the above simulation results, the feasibility of the security architecture proposed in this paper is relatively high, less performance impact, greater security upgrade. Currently due to time reasons, only the performance evaluation under black hole attack, more attack scenarios will be added gradually for the evaluation of the architecture performance of different scenarios which are expected to more detailed and further optimized.

References

[1] Trusted Computing Group. *http://www.trustedcomputinggroup.org/developers /trusted_platform_module.*

[2] Trusted Computing Group. “TCG Trusted Network Connect TNC Architecture for Interoperability,” Specification Version 1.5 Revision 3, 2012. *http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications*.

[3] Sadeghi A R, Stuble C. Property-based attestation for computing platforms: caring about properties, not mechanisms.*NSPW’04:Proceedings of the 2004 Workshop on New Security Paradigms*.2004:67-77.

[4] Petroni N L Jr, Hicks M. Automated Detection of Persistent Kernel Control-Flow Attacks. *Computer and Communications Security* (CCS’07), Alexandria, Virginia, October 2007:103-115.

[5] Shi E, Perring A, van Doorn L. BIND: A Fine-grained Attestation Service for Secure Distributed Systems. *IEEE Symposium on Security and Privacy* (S&P05).2005:154-168.

[6] Xu Wen-juan,Zhang Xin-wen, Hu Hong-xin,et al. Remote Attestation with Domain-based Integrity Model and Policy Analysis. *IEEE Transactions on Dependable and Secure Computing,* 2011:61.

[7] Ali T, Nauman M, Zhang Xin-wen. On Leveraging Stochastic Models for Remote Attestation. *Proceedings of INTRUST*.2010:290-301.

[8] Brickell, E.F, Camenisch, J. and Chen L. 2004. Direct anonymous attestation. *In ACM Conference on Computer and Communications Security*, 132-145