PROCEEDINGS OF SCIENCE

Security Analysis of GRID Protocol for MANET Based on BAN Logic

Shuai Han[1]
Army Engineering University
Hebei, 050003, China
E-mail: hanshuai0323@126.com

Wencheng Jiao[2]
Army Engineering University
Hebei, 050003, China
E-mail: jiaowc@163.com

The security of GRID routing protocol based on location information in mobile Ad Hoc networks needs to be verified, so a formal method is introduced to achieve this goal in this paper. Based on BAN logic, this method also combines the characteristics of Ad Hoc network routing protocal. The analysis results show that the protocol has security vulnerabilities in the route maintenance phase which cannot be pinpointed. From the analysis results, this method is proved to be effective and lay the foundation for the improvement of GRID protocol in the future.

ISCC2017
16-17 December 2017
Guangzhou, China

[1]Shuai Han(1994-), master graduate student, research for the network information security.
[2]Wencheng Jiao(1970-), associate professor, research for software support, information security and countermeasure.

© *Copyright owned by the author(s) under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0).*

PoS(ISCC 2017)042

1.Introduction

Mobile Ad Hoc network is a group of mobile nodes with wireless devices autonomous network. The GRID protocol [1] is a complete routing protocol based on location information. The location information is used to solve three key problems: finding routes, forwarding data packets and maintaining routes. The routing protocol security is the basis of the entire network security. The adoption of formal methods in recent years has found a flaw in the protocol that has never been discovered before, and thus attracts more and more attention. Formal analysis is a comprehensive and effective way to test the security of protocols. The BAN logic [2] is a milestone in analyzing security protocols proposed by Burrows, Abadi and Needham. It is a logic analysis based on knowledge and belief. Through the reception and sending of messages during the operation of the authentication protocol, it gradually evolves from the initial belief to the goal of agreement operation.

At present, the analysis of security protocols mainly adopts informal methods mainly relying on the subjective experience of analysts. However, it is difficult to find some hidden defects and vulnerabilities. Ying-Long Wang [3] and others used BAN logic to verify the security-aware adaptive DSR (SADSR) protocol and provided a method reference.

In recent years, few scholars have verified the safety of GRID routing protocol by formal analysis. Therefore, this paper combines the characteristics of Ad Hoc networks to reasonably formalize the routing protocols. This article firstly introduces the BAN logic analysis method, then briefly explains the GRID routing protocol, and shows how it is used based on BAN logic. Finally, draw the conclusion.

2. BAN Logic

BAN logic objects include Principals, Keys, and Formulas. Formulas are also known as Statement Live statements. In general, P,Q and R represent the main variables, K represents the key variable, X and Y represent the formula variables. Let A and B denote two common subjects and S indicate the authentication server, $N_{A\ and}$ N_B represent random number respectively. K_{AB}, K_{AS} and K_{BS} represent the shared keys, K_A and K_B indicate publice keys and K_A^{-1} and K_B^{-1} are the corresponding private keys. H(X) represents a one-way hash function of X.

2.1 Symbol

The BAN logic contains a conjunction, as expressed in the commas; in addition, it defines the following logical notation:

$P \mid\equiv X$:P trust X; (2.1)

$P \lhd X$:P see X; (2.2)

$P \mid\Rightarrow X$:P has the right to arbitrate X; (2.3)

$\#(X)$:X is new; (2.4)

$P \overset{k}{\leftrightarrow} X$:K is P, Q's shared key; (2.5)

$\overset{K}{\mapsto} P$:K is P's public key; (2.6)

$P \overset{X}{\leftrightarrows} Q$:X is the shared secret between P and Q; (2.7)

PoS(ISCC 2017)042

$\{X\}_K$:Encrypting X using a key K; (2.8)

$\langle X \rangle_Y$:X is keep secret with secret Y. (2.9)

What needs special attention here is that P once said that X did not mean P believed X.

2.2 Rules

There are almost 19 rules of BAN logic, the commonly uesed are as follows:

R1: $$\frac{P \mid \equiv Q \overset{k}{\leftrightarrow} P,\ P \lhd \{X\}_k}{P \mid \equiv Q \mid \sim X}$$

If P believes K is a shared key of P and Q, and P has received message $\{X\}_K$ encrypted with K, P believes that Q has sent message X.

Similarly, in case of a public key and a shared secret, the following inference rules R_2.

R2: $$\frac{P \mid \equiv Q \overset{k}{\rightarrow} P,\ P \lhd \{X\}_{k^{-1}}}{P \mid \equiv Q \mid \sim X}$$

R3: $$\frac{P \mid \equiv \#(X), P \mid \equiv Q \mid \sim X}{P \mid \equiv Q \mid \equiv X}$$

If P believes fresh X, P believes Q have transmitted X, then P believes that Q believes X.

R4: $$\frac{P \mid \equiv Q \mid \Rightarrow X,\ P \mid \equiv Q \mid \equiv X}{P \mid \equiv X}$$

If P believes Q has to arbitration for X, P believes that Q believes X, then P believes X.

R5: $$\frac{P \mid \equiv Q \mid \sim (X, Y)}{P \mid \equiv Q \mid \sim X}$$

If P believes Q has sent a message (X, Y), P believes that Q has sent the message X.

R6: $$\frac{P \mid \equiv \#(X)}{P \mid \equiv \#(X, Y)}$$

If P believes X is fresh, P believes that (X, Y) is also fresh.

According to Ad Hoc network routing protocol features, we demand to add a rule:

R7: $$\frac{P \mid \equiv X,\ P \mid \equiv R \mid \equiv (X, R)}{P \mid \equiv (X, R)}$$

If P believes that R believes the message (X, R), P believes that R forwards message X and adds its own address R, P believes X, so P believes (X, R).

3.GRID Routing Protocol Security Analysis

3.1 Analytical Method

To analyze the security of the routing protocol, the method is based on the BAN logic general analysis of the protocol and combined with the characteristics of MANET route protocol . This method is shown as follows:

3.1.1 Analysis Steps

The general steps for analyzing protocols using BAN logic are as follows:

PoS(ISCC 2017)042

1) Formalize the protocol according to the rules of BAN logic;

2) Determine the protocol's initial assumptions and security goals, and use logical notation to represent;

3) Establish the initial logic inference rules and assumptions, for each message protocol reasoning, if the introduction of security objectives, the protocol in this method is safe, otherwise it is unsafe, then analyze the defects and redundancy of protocol according to reasoning process,.

3.1.2 Agreement Formalized

MANET routing protocols can be divided into two basic sub-protocols: the route discovery sub-protocol and the route maintenance sub-protocol. In addition, in some routing protocols, such as ARAN [4], neighboring nodes need to authenticate each other. Therefore, the entire routing protocol can be divided into the following three sub-protocols:

Sub-protocol 1: Authentication of neighboring nodes and node and server authentication

A->B: Message1

B->A: Message2

Sub-protocol 2: Route discovery process

In some routing protocols, such as DSR [5], in addition to the destination node which sends a route response message, the intermediate node can also send the routing response message. Therefore, the route discovery sub-protocol may be further divided into the following two sub-protocols:

Sub-protocol 2.1: The destination node replies with the message

A->Router1: Message3

Router1->Router2: Message4

Router2->B: Message5

B->Router2: Message6

Router2->Router1: Message7

Router1->A: Message8

A->B: Data

B->Router2: Message9

Router2->Router1: Message10

Router1->A: Message11

Subprotocol 2.2: The intermediate node replies to the routing packet

A->Router1: Message3

Router1->Router2: Message4

Router2->Router1: Message12

Router1->A: Message13

A->B: Data

B->Router2: Message9

Router2->Router1: Message10

Router1->A: Message11

Subprotocol 3: Routing maintenance process

Router2->Router1: Message14

Router1->A: Message15

In the above formalization, A represents the source node, B represents the destination node, and Router 1 and Router 2 (hereinafter abbreviated as R1 and R2) represent intermediate nodes. In the actual routing process, the number of intermediate nodes is uncertain, but the

PoS(ISCC 2017)042

messages they send are formally consistent, so they need not be formally expressed in terms of their form. Considering the generality of the routing process and analysis of the convenience, the number of intermediate nodes in the formalization reduced to two. Data in Subprotocol 2 indicates that the routing protocol sends encapsulated upper layer protocol packets.

The specific routing protocol does not necessarily include all three sub-protocols, only consider the security of the sub-protocol used when analyzing its security.

3.1.3 Safety Goals

The general form of security objectives in BAN logic is as follows:

$$A \mid\equiv X,\ B \mid\equiv X,\ A \mid\equiv B \mid\equiv X,\ B \mid\equiv A \mid\equiv X$$

According to the different purposes of each sub-agreement, their corresponding security goals are also different. For the subprotocols 2 and 3, the route discovery and maintenance process, if path information appears in the routing protocol packet, the formula X is A, R1, R2, B; if path information does not appear in the message, X is a hop count or a random number N.

For Subprotocol 1 the authentication between nodes, does not require verification, and the security goal can be defined as follows:

$$A \mid\equiv B \mid\overset{K_a}{\rightarrow} A,\ B \mid\equiv A \mid\overset{K_b}{\rightarrow} B$$

3.2 Formal Analysis of GRID Protocol

The formal methods are used in the following GRID protocol for security verification. GRID protocol borrows the basic procedure of route discovery and route maintenance in AODV protocol [6]. There are three types of control frames: RREQ, RREP, and RERR. Two important protocols are Path Discovery and Route Request. The intermediate forwarding node is a gateway selected by the gateway selection protocol and performs an intermediate forwarding operation. Only the node that becomes a gateway of the mesh needs to process and forward the request packet related to the routing.

3.2.1 Formal

The GRID contains only Sub-protocols 2.1 and 3. The authentication of a node is performed offline and the intermediate node cannot send routing reply packets. To verify the validity of the above method, it is assumed that Sub-protocol 1 and Sub-protocol 2.2 are also used in GRID. The messages in subprotocol 1 adopt authenticated routing for ad hoc networks (ARAN). The messages in Subprotocol 2.2 are constructed according to the messages in GRID. The specific form is as follows:

Message1: $\{K_s, T_a\} K_a^{-1}$

Message2: $\{K_s, A, K_a\} K_s^{-1}$

Message3: $A, T_a, \{\{A, T_a\} K_h\} K_a^{-1}, \{K_s, A, K_a\} K_s^{-1}$

Message4: $A, R1, T_a, \{\{A, T_a\} K_h\} K_a^{-1}, \{K_s, A, K_a\} K_s^{-1}, \{\{A, R1, T_a\} K_h\} K_{r1}^{-1}, \{K_s, R1, K_{r1}\} K_s^{-1}$

PoS(ISCC 2017)042

$$A, R1, R2, T_a, \{\{A, T_a\} K_h\} K_a^{-1}, \{K_s, A, K_a\} K_s^{-1},$$

Message5: $\{\{A, R1, T_a\} K_h\} K_{r1}^{-1}, \{K_s, R1, K_{r1}\} K_s^{-1},$
$\{\{A, R1, R2, T_a\} K_h\} K_{r2}^{-1}, \{K_s, R2, K_{r2}\} K_s^{-1}$

Message6: $A, R1, R2, B, T_a, \{\{A, R1, R2, B, T_a\} K_h\} K_b^{-1}, \{K_s, B, K_b\} K_s^{-1}$

Message7: $A, R1, R2, B, T_a, \{\{A, R1, R2, B, T_a\} K_h\} K_b^{-1}, \{K_s, B, K_b\} K_s^{-1},$
$\{\{A, R1, R2, B, T_a\} K_h\} K_{r2}^{-1}, \{K_s, R2, K_{r2}\} K_s^{-1}$

$$A, R1, R2, B, T_a, \{\{A, R1, R2, B, T_a\} K_h\} K_b^{-1}, \{K_s, B, K_b\} K_s^{-1},$$

Message8: $\{\{A, R1, R2, B, T_a\} K_h\} K_{r2}^{-1}, \{K_s, R2, K_{r2}\} K_s^{-1},$
$\{\{A, R1, R2, B, T_a\} K_h\} K_{r1}^{-1}, \{K_s, R1, K_{r1}\} K_s^{-1}$

Message9: $R2, R1, A, N_b, \{\{R2, R1, A, N_b\} K_h\} K_b^{-1}, \{K_s, B, K_b\} K_s^{-1}$

Message10: $R2, R1, A, N_b, \{\{R2, R1, A, N_b\} K_h\} K_b^{-1}, \{K_s, B, K_b\} K_s^{-1},$
$\{\{R2, R1, A, N_b\} K_h\} K_a^{-1}, \{K_s, A, K_a\} K_s^{-1}$

$$R2, R1, A, N_b, \{\{R2, R1, A, N_b\} K_h\} K_b^{-1}, \{K_s, B, K_b\} K_s^{-1},$$

Message11: $\{\{R2, R1, A, N_b\} K_h\} K_a^{-1}, \{K_s, A, K_a\} K_s^{-1},$
$\{\{R2, R1, A, N_b\} K_h\} K_{r2}^{-1}, \{K_s, R2, K_{r2}\} K_s^{-1},$
$\{\{R2, R1, A, N_b\} K_h\} K_{r1}^{-1}, \{K_s, R1, K_{r1}\} K_s^{-1}$

Message12: $A, R1, R2, B, T_a, \{\{A, R1, R2, B, T_a\} K_h\} K_{r2}^{-1}, \{K_s, B, K_{r2}\} K_s^{-1}$

Message13: $A, R1, R2, B, T_a, \{\{A, R1, R2, B, T_a\} K_h\} K_{r2}^{-1}, \{K_s, B, K_{r2}\} K_s^{-1},$
$\{\{A, R1, R2, B, T_a\} K_h\} K_{r1}^{-1}, \{K_s, B, K_{r1}\} K_s^{-1}$

Message14: $R2, R1, A, T_{r2}, \{\{R2, R1, A, T_{r2}\} K_h\} K_{r2}^{-1}, \{K_s, R2, K_{r2}\} K_s^{-1}$

Message15: $R2, R1, A, T_{r2}, \{\{R2, R1, A, T_{r2}\} K_h\} K_{r1}^{-1}, \{K_s, R1, K_{r1}\} K_s^{-1}$

3.2.2 Initial Assumption

Since the management of keys in GRID takes an off-line approach, the following assumptions and freshness assumptions can be made:

$$A \mid\equiv \mid\xrightarrow{k} S ; A \mid\equiv S \mid\Rightarrow K_i, i=a, r1, r2, b ; A \mid\equiv \#(K_i), i=a, r1, r2, b ; A \mid\equiv \#(T_a)$$

$$R1 \mid\equiv \mid\xrightarrow{k} S ; R1 \mid\equiv S \mid\Rightarrow K_i, i=a, r1, r2, b ; R1 \mid\equiv \#(K_i), i=a, r1, r2, b ; R1 \mid\equiv \#(T_a)$$

$$R2 \mid\equiv \mid\xrightarrow{k} S ; R2 \mid\equiv S \mid\Rightarrow K_i, i=a, r1, r2, b ; R2 \mid\equiv \#(K_i), i=a, r1, r2, b ; R2 \mid\equiv \#(T_a)$$

$$B \mid\equiv \mid\xrightarrow{k} S ; B \mid\equiv S \mid\Rightarrow K_i, i=a, r1, r2, b ; B \mid\equiv \#(K_i), i=a, r1, r2, b ; B \mid\equiv \#(T_a)$$

3.2.3 Analysis and Reasoning

PoS(ISCC 2017)042

According to the assumptions and rules, respectively, all the reasoning of the news is listed as follows:

For Message1:

$$\frac{S \mid\equiv \overset{k_a}{\mapsto} A \quad S \lhd \{K_s, T_a\} K_a^{-1} \qquad S \mid\equiv A \mid\sim K_s, T_a \quad S \equiv \#(T_a)}{S \mid\equiv A \mid\equiv \overset{k_s}{\mapsto} S}$$

Corresponding, for Message2: $A \mid\equiv S \mid\equiv \overset{k_a}{\rightarrow} A$

For Message3:

$$\frac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{R1 \mid\equiv \overset{K_s}{\mapsto} S, R1 \lhd \{K_s, A, K_a\} K_s^{-1}}{R1 \mid\equiv S \mid\sim K_s, A, K_a} \qquad R1 \mid\equiv S \mid\equiv \xrightarrow{K_a} A, R1 \mid\equiv S \mid\Rightarrow K_a}{R1 \mid\equiv \xrightarrow{K_a} A, R1 \lhd \{\{A, T_a\} K_h\} K_a^{-1}}}{R1 \mid\equiv A \mid\sim \{A, T_a\} K_h, R1 \mid\equiv \#(T_a)}}{R1 \mid\equiv A \mid\equiv \{A, T_a\} K_h}}{R1 \mid\equiv \{A, T_a\} K_h}}{R1 \mid\equiv A}$$

And so on, Message5 can be drawn $B \mid\equiv A, B \mid\equiv R1 \mid\equiv A, R1$, so:

$$\frac{B \mid\equiv A \quad B \mid\equiv R1 \mid\equiv A, R1}{B \mid\equiv A, R1 \quad B \mid\equiv R2 \mid\equiv A, R1, R2}$$
$$B \mid\equiv A, R1, R2, B$$

Corresponding, for Message8: $A \mid\equiv A, R1, R2, B; A \mid\equiv B \mid\equiv A, R1, R2, B$. When B receives Data, it can be drawn $B \mid\equiv A \mid\equiv A, R1, R2, B$. For Message11: $A \mid\equiv B \mid\equiv A \mid\equiv A, R1, R2, B$.

For the intermediate node to reply to the routing packet, similarly, for Message 13: $A \mid\equiv A, R1, R2, B$. When B receives data, it can be drawn $B \mid\equiv A \mid\equiv A, R1, R2, B$. For Message 11: $A \mid\equiv B \mid\equiv A \mid\equiv A, R1, R2, B$. When B receives Data again, it can be drawn $B \mid\equiv A, R1, R2, B$.

For routing maintenance process, Message 15：
$A \mid\equiv R2, R1, A; A \mid\equiv R2 \mid\equiv R2, R1, B$.

3.2.4 Analysis Results

From the above analysis we can see:

1) The hash key K_h and digital certificates K_s have no effect on the security of the protocol. During the routing reply, the digital signature of the intermediate node does not contribute to the security. Therefore, it is assumed that the sub-protocol 1 and sub-protocol 2.2 existing in GRID do not affect formal analysis.

2) The authentication between nodes is safe under this method and achieves the safety goals.

3) For the route discovery process, we can draw

$A \mid\equiv A, R1, R2, B; B \mid\equiv A, R1, R2, B$

$A \mid\equiv B \mid\equiv A, R1, R2, B; B \mid\equiv A \mid\equiv A, R1, R2, B$

PoS(ISCC 2017)042

The intermediate node replying to the routing request does not affect the security of the protocol, so it is entirely possible to allow the intermediate node to reply to the routing request.

Routing maintenance process can only be drawn

$A \mid\equiv R2, R1, A; A \mid\equiv R2 \mid\equiv R2, R1, A$, cannot be drawn

$R2 \mid\equiv R2, R1, A; R2 \mid\equiv A \mid\equiv R2, R1, A$.

In summary, the Subprotocols 1 and 2 in the GRID protocol are secure under this method, and the subprotocol 3 route maintenance process is insecure. Therefore, the GRID protocol is insecure. But the method cannot clearly point out the defects of the agreement, it remains necessary to find a more specific and intuitive method of agreement loopholes.

4.Conclusion

From the above analysis we can see that, for the security analysis of GRID routing protocol, BAN logic method can give a rigorous mathematical reasoning, but there are many deficiencies in this method. Because this method uses proof method, for unsafe routing protocols, we cannot figure out the cause of the loopholes even if we can prove their existence. So the improvement of the unsafe protocol still need to rely on the designer's experience. Since BAN logic analysis can only certify the agreement, this method only analyzes the source node and the destination node information on the likelihood of agreement, but cannot analyze confidentiality of the information. The next step is to use more advanced analytics, such as using the attacker model to find the attack path, facilitate accurate finding of protocol defect locations, and facilitate g improvements in unsafe protocols.

References

[1] Liao Wen-Hwa, Sheu Jang-Ping, Tseng Yu-Chee. GRID: *A Fully Location-Aware Routing Protocol for Mobile Ad Hoc Networks*[J]. Telecommunication Systems, 2001, 18(1): 37-60.

[2] BURROWS M, ABADI M, *NEEDHAM R. A Logic of Authentication*[R]. SRC Research Report 39, 1989.

[3] Ying-long WANG, Ji-Zhi WANG, Mei-Qin WANG. *Security analysis of routing protocol for MANET based on BAN logic*[J]. Journal of China Institute of Communications, 2005, 26(4): 125-129 (In Chinese)

[4] KIMAYA S, BRIDGET D, et al. *A Secure Routing Protocol for Ad Hoc Networks*[R]. Technical Report 01-37, Department of Computer Science, University of Massachusetts, August 2001.

[5] JOHNSON D B, MALTZ D A, HU Y C. *The dynamic source routing protocol for mobile ad hoc networks(DSR)[EB/OL]*. http://www.ietf.org/ internet-drafts/draft-ietf-manet-dsr-09.txt.

[6] Perkins C, Belding Royer E, Das S. *Ad-hoc On-demand distance vector (AODV) routing* [M]. RFC Editor, 2003.

PoS(ISCC 2017)042