OTNA: One Time Node Authentication for Secure MANET

Komal Naik (Joshi)
Student
Computer Engineering Department, PVPIT,
Savitribai Phule Pune University[2], Pune, India

Arati M. Dixit[1,2]
Computer Engineering Department, PVPIT[1], Pune
Department of Technology, Savitribai Phule Pune
University[2], Pune, India

ABSTRACT

Due to infrastructure – less networks and multi - hop communication features of Mobile ad hoc network (MANET), every node in MANET has to cooperate with each other. Therefore, node security becomes one of the important research areas of MANET. The resources that provided to MANET nodes such as battery power, memory, and bandwidth are limited. As a result, developing a resource – aware node authentication protocol becomes challenge for researchers. The proposed protocol provides One Time Node Authentication (OTNA) for every node joining MANET. To achieve this, the OTNA protocol provides one additional field 'status' in the routing table of the legitimate nodes, and the Malicious Node Table (MNT). The 'status' field shows authentication status of the nodes present in MANET. The MNT is used to keep record of the malicious nodes detected during node authentication. To perform node authentication, OTNA uses the basics of Challenge - Response Protocol (CRP) and one-way hash function with three message exchanges. In the OTNA protocol, only two nodes are involved in authentication process, which allows other available nodes for packet forwarding process. To the best of our knowledge, OTNA protocol facilitates optimal secure packet delivery. The correctness of the OTNA protocol is proved with the help of GNY logic.

General Terms

Wireless Sensor networks (WSN) and Mobile ad-hoc network (MANET), Security in MANET.

Keywords

MANET, Node Authentication, Challenge-Response protocol, GNY Logic.

1. INTRODUCTION

Mobile ad hoc network (MANET) is a collection of mobile nodes that are connected to each other by means of wireless links. A node can join or leave the network at any instance. A node in MANET can act as a router and also as a host. For packet forwarding in MANET several routing protocols are developed. Routing in MANET is based on Route request (RREQ) and Route Response (RRES) control packets used for path discovery process. Because of infrastructure - less and multi - hop communication features of MANET, every node in MANET has to cooperate with each other. Therefore, node security becomes one of the important research areas of MANET. Also MANETs are wireless mobile networks; hence resources provided to MANET nodes such as battery power, memory and bandwidth are limited. As a result, developing resource – aware node authentication protocol becomes challenge for researchers.

A node authentication in MANET is a process that involves one or multiple legitimate nodes who provides authentication to the requestor node by means of specific authentication protocol. There are basically two types of node authentication techniques present for MANET; certificate based node authentication [1] and trust relationship based node authentication [2]. Various protocols are developed based on these two node authentication techniques. The Certificate based node authentication uses certificates exchange between legitimate nodes present in the network to authenticate a requestor node. As a legitimate node receives a certificate request for requestor node from other legitimate nodes in network, it has to provide requested certificate for authentication process. Then based on the number of received certificates from other legitimate nodes in MANET, an authentication can be provided to the requestor node. In trust relationship based authentication, trust relationship can be developed based on some predefined threshold values or by exchanging certain secret messages in the network.

The challenge - response protocol (CRP) [3] is based on sharing secrets between two entities. The proposed One Time Node Authentication (OTNA) protocol consider node as an entity. In CRP, one node sends a secret question as challenge to other node and generates answer. Other node also has to generate answer for the same question and then the node that sends a challenge will make the verification.

Based on this idea, a combination of dynamically generated CRP - key and a secure hash algorithm is used to perform node authentication process in the proposed protocol. So that resources required for computing node authentication process will be reduced. The proposed protocol provides one time node authentication for every node in MANET. To achieve this, the OTNA protocol provides one additional field 'status' in the routing table of the legitimate nodes, and the Malicious Node Table (MNT). The status field shows authentication status of the nodes present in MANET. The MNT is used to keep record of the malicious nodes detected during node authentication. The routing table information and MNT information helps to keep track of authentication status of particular node. The objective of proposed approach is to prevent MANET from unauthorized node's access in MANET and to provide resource aware node authentication protocol. The objectives are achieved by using a CRP and one way hash function, which uses three message exchanges, MNT and 'status' field in the routing table of legitimate nodes to perform node authentication. The OTNA protocol uses less number of message exchanges, which in turn reduces control overhead during node authentication process. Another strong feature of OTNA is that only two nodes are involved in authentication process, which allows other available nodes for packet forwarding process.

The rest of paper is organized as follows: section 2 presents current related research to perform node authentication in MANET. In section 3, the OTNA protocol is proposed. The OTNA protocol's correctness proof is illustrated using GNY logic in section 4. Finally the conclusions are given in the last section.

2. RELATED WORK

According to features of MANET, a node security plays important role. A node authentication must be performed to secure a node in MANET. There are basically two types of node authentication techniques present; certificate based authentication and trust relationship based authentication. Based on these two techniques various protocols are developed by various researchers.

Nikos Komninos et al. used the challenge response protocol and zero knowledge protocol for node's validity in network [5]. In this work, a non-interactive zero knowledge protocol used to determine the true identity of the communicating nodes and a challenge-response protocol used to perform node authentication of communicating nodes. The main problem with this method is control overhead increases due to multiple packets used for node authentication. H Deng et al. have used concept of Identity-based cryptography and threshold secret sharing for distributed key management and authentication [6]. Authors have used self-organizing way to provide key generation and key management service instead of using traditional prefixed trust relationship between nodes. In this scheme authors avoid centralized certificate authority to distribute public keys and certificates which saves network bandwidth and reduces network overhead [6]. A threshold cryptography- based key management scheme for MANETs have been proposed Zhou et al. [7]. In this scheme, a certificate authority (CA) provides a master public/private key pair to the group of n servers. Each server is provided by a share of the master private key and has to keep record of the key pairs of all nodes. The threshold cryptography is used to generate the shares of the master private key. Therefore only n servers together can form a complete signature. If any node wishes to join the network, it first has to collect all of the n partial signatures and then by computing the complete signature locally, it can get the certificate. Kong et al. has extended this scheme by providing a centralized dealer, to issue certificates and private key shares to 't' nodes during the network bootstrapping phase [8]. A statistically unique and cryptographically verifiable (SUCV) identifier scheme has been proposed by Montenegro et al. In this scheme every node is responsible to compute their address. The addresses are computed by applying a non - reversible hash function on their public key [9].Then any node can directly bind a public key to its owner address. This scheme prevents IP spoofing and provides a reliable authentication scheme for the nodes in a MANET.

A trust establishment mechanism has been proposed by Eshenaur et al.[10]. In this mechanism any node in the network can generate trust evidence about other node in a MANET. A principal node generates a piece of trust evidence for other node with a specific lifetime, the principal node signs the newly generated evidence with its own private key, and makes the newly generated evidence available to others through the network. A piece of evidence is revoked by using a revocation certificate and makes it available to others at any time within its specified lifetime. After distributing a trust evidence, a principal can get disconnected. Similarly, a requestor of trust evidence does not have to be reachable at the time its evidence is being computed. Evidences can be broadcasted across various nodes to guarantee availability. Although the scheme is conceptually sound, the authors have not provided any details about the performance evaluation of the scheme. A distributed trust model has been proposed by Abdul- Rahman et al. [11]. In this scheme a decentralized trust management approach is used. This recommendation protocol to exchange trust-related information. The model assumes that two nodes are connected by unidirectional relationships. The nodes uses their policies to make judgments about the quality of a recommendation of trust. The recommendation protocol is based on requesting a trust value in a trust target with respect to a specific classification and analyzing it's an answer. Then an overall trust value can be evaluated by using evaluation function at the target node. A trust management scheme for self-organized ad hoc networks has been proposed by Baras et al. [12]. In this scheme the nodes share trust information only with their neighbors. A voting mechanism has been proposed for establishing and maintaining trust among the neighbors by the authors. This voting mechanism has made the scheme robust. A self-organized trust establishment scheme has been proposed by Sen et al. for nodes in a large-scale MANET. In this scheme a trust initiator is introduced during the network bootstrapping phase [13]. The authors have also proposed a distributed trust-based intrusion detection system for MANETs based on cooperation among nodes [14]. Authors Marjan et al have proposed a two phase detection scheme to select a monitoring node for intrusion detection system amongst the authorized nodes present in MANET[15]. The authors have used a non interactive zero knowledge protocol to detect authorized nodes present in MANET. Then voting mechanism used to select monitoring node. The selection of monitoring node based on number of votes and largest battery power the node having. Need to perform selection of monitoring node again and again if battery power decreases rapidly; as monitoring node has to perform many operations.

In certificate based node authentication techniques, every node has to maintain a certificate repository and whenever request arrives for certificate of particular node, it has to provide certificate of respective node. Therefore every node consumes certain memory to keep certificate repository. Moreover the certificate exchange increases communication overhead in the network. In trust based node authentication techniques, it is necessary that participating nodes must have a close contact between each other. Establishing trust increases battery consumption. Again in both techniques there is no provision to keep authentication status of every authenticated node present in network. Therefore it is necessary to perform node authentication again and again.

Therefore, the One Time Node Authentication (OTNA) Protocol is proposed to overcome limitations of existing node authentication techniques. The proposed protocol provides one time node authentication for every node in MANET using CRP and One-way hash function.

3. THE OTNA PROTOCOL

The proposed protocol provides one time node authentication for every node in MANET. To achieve this, the OTNA provides one additional field 'status' in the routing table of the legitimate nodes, and the Malicious Node Table (MNT).

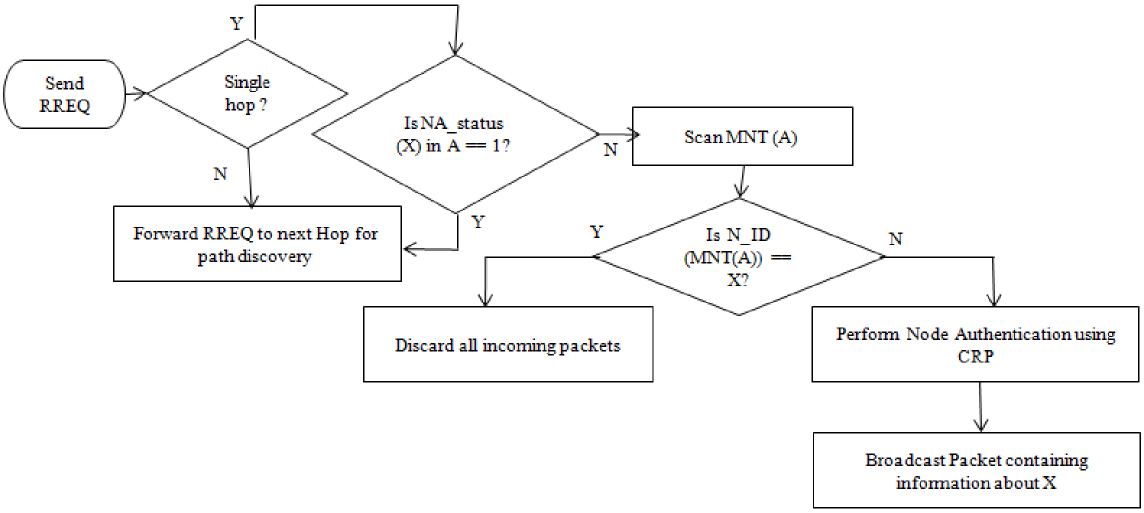
Send RREQ
Single hop ?
Y
N
Is NA_status (X) in A == 1?
N
Y
Forward RREQ to next Hop for path discovery
Scan MNT (A)
Is N_ID (MNT(A)) == X?
Y
N
Discard all incoming packets
Perform Node Authentication using CRP
Broadcast Packet containing information about X

Fig 1: OTNA protocol: System flow

The status field shows authentication status of the nodes present in MANET. The MNT is used to keep record of the malicious nodes detected during node authentication. To perform node authentication, OTNA uses the basics of CRP and one-way hash function. The routing table information and MNT information helps to keep track of authentication status of particular node.

3.1 OTNA Protocol: System Flow

The system flow of OTNA protocol is shown in Fig.1 The protocol initiates with the RREQ recieved by other node. As shown in Fig. 2, the OTNA protocol uses following message exchange sequences:

1. New node : send RREQ for validity in network.
2. Legitimate node: Check new node's entry in routing table's 'status' feild and in MNT.
3. Legitimate node: either forward RREQ to next hop, if new node's status in routing table is '1'. Or send CRPK as a secret message to new node for authentication process.
4. New Node and Legitimate node : generate answer using hash function.
5. New Node: send answer to legitimate node.
6. Legitimate node: Compare answer.
7. Legitimate node: if answer is same then declare new node as legitimate node, else declare new node as malicious node.
8. Broadcast respective information about new node in the network.

3.2 OTNA Protocol: Components

The components of the OTNA protocol [20] can be seen Fig. 3. The OTNA protocol includes; Node Authentication Unit (NAU), Malicious Node Table (MNT), Broadcast Unit (BU), Path Discovery Unit (PDU), Packet Forwarding Unit (PFU). The NAU is responsible to authenticate a newly join node in MANET. The NAU initiates if the status of the requestor node in the routing table of the legitimate node is 0. Then it uses CRP and one-way hash function for authenticating a node. Based on the authentication status detected by NAU, the BU will broadcast a data packet containing information about the requestor node. The BU is also responsible to broadcast a RREQ control packet. The MNT is responsible to maintain information about malicious node detected by NAU; The PDU is responsible to discover a secure path for data packet forwarding using a routing protocol and information kept in MNT from source node to destination node. During path discovery the PDU scans MNT for verifying that the intermediates nodes are legitimate nodes or malicious nodes. The PFU uses a path discovered by PDU to forward a data packet from source node to destination node.

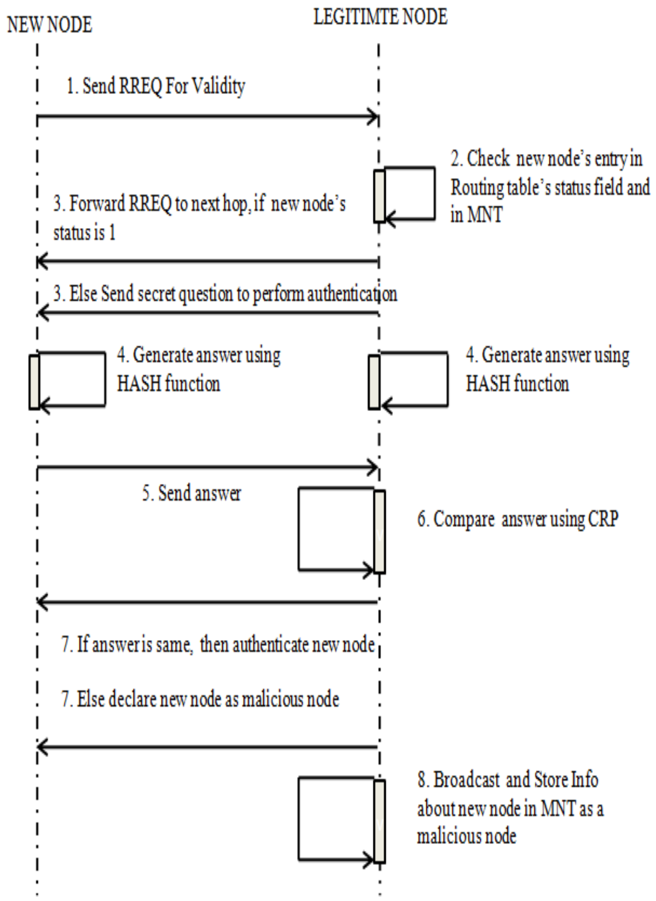
NEW NODE
LEGITIMTE NODE
1. Send RREQ For Validity
2. Check new node's entry in Routing table's status field and in MNT
3. Forward RREQ to next hop, if new node's status is 1
3. Else Send secret question to perform authentication
4. Generate answer using HASH function
4. Generate answer using HASH function
5. Send answer
6. Compare answer using CRP
7. If answer is same, then authenticate new node
7. Else declare new node as malicious node
8. Broadcast and Store Info about new node in MNT as a malicious node

Fig. 2 OTNA protocol: Sequences performed

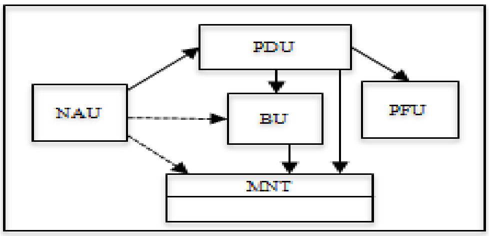

Fig. 3 OTNA protocol: Components

3.3 Algorithm

The OTNA protocol performs node authentication for every node present in MANET only once. The protocol initiates with the RREQ received by other node. Algorithm 1 describes algorithm for OTNA protocol. Consider ‘N1’ is a legitimate node and ‘N2’ is a new node in MANET. ‘N1’ receives RREQ from ‘N2’. Then ‘N1’ checks whether received RREQ is first RREQ or not. If RREQ is not a first RREQ then ‘N1’ forward RREQ to its next-hop for path discovery process. If RREQ is a first RREQ then ‘N1’ will check ‘N2’ node’s status in the ‘status’ field of N1’s routing table. If $N1(RTStatus(X)) = 1$, then ‘N2’ is authenticated node and forward RREQ to next-hop for path discovery. If status is ‘0’, then ‘N1’ will scan its MNT for entry of ‘N2’. If MNT(NodeName) = N2 i.e ‘N2’ is present in MNT; it means authentication for ‘N2’ is done previously and was declared as malicious node. If ‘N2’ is not present in MNT then go to Algorithm 2 for node authentication.

Algorithm 1 Initialization and data packet forwarding in OTNA

Input: N2 = new node , N1 = legitimate node in MANET, RREQ= Route Request, MNT(NodeName) = Malicious node table, N1(RTStatus) = Routing table’s status field

```
$N1 \leftarrow RREQ(X)$          // ‘N1’ receives RREQ from N2
‘N1’ checks its routing table’s status field for N2’s validity in the network.
if $N1(RTStatus(X)) = 1$ then
    Then proceed RREQ for route discovery
else
    Check entry of N2 in MNT
    if MNT(NodeName) = N2 then
        discard all incoming packets from N2
    else
        call algorithm 2        // perform Node authentication
    end if
end if
```

In Algorithm 2, both nodes will be engaged to perform authentication process. The authentication process is based on CRP. ‘N1’ will generate a ι – bits long random CRP-Key (CRPK) *i.e* $N1 : CRPK \leftarrow \{0,1\}ι$. And send it to ‘N2’ as a $(M1) = (CRPK)$ secret question. Then ‘N1’ and ‘N2’ generate hash value for CRPK using a secure hash algorithm as $(M2)_H$ and $(M3)_H$. ‘N2’ send $(M3)_H$ to ‘N1’ as a response. ‘N1’ will compare answer. If $(M2)_H = (M3)_H$, then $N1 \rightarrow * : <LN>$, i.e ‘N1’ will declare ‘N2’ as legitimate node. Else $N1 \rightarrow * : <MN>$, i.e ‘N1’ will declare ‘N2’ as malicious node. ‘N1’ will broadcast a data packet containing information about ‘N2’ and Set $(RTStatus(N2) = 0)$.

4. OTNA PROTOCOL CORRECTNESS PROOF

The authentication process involves message exchange between the participating entities and for this must have belief on each other. The correctness of cryptographic authentication protocols is proved by using a logic-based approach for authentication. This approach is based on the use of logics of belief and/or knowledge. This approach provides certain inference rules which can be applied to some assumptions and message exchanges of the protocol to derive the protocol goals. Different logic-based approaches are available such as BAN Logic, GNY Logic, RV Logic, AT Logic, VO Logic, SVO Logic and MAO Logic [18, 19]. Among these logics, the GNY is used to prove correctness of OTNA protocol.

Algorithm 2 CRP based Node Authentication in OTNA Protocol

Inputs: N2 is new node, N1 is legitimate node in MANET. M_n = Messages

```
$N1 : CRPK \leftarrow \{0,1\}ι$      // node ‘N1’ takes ι - bit long dynamically generated CRP key.
$(M1) = (CRPK)$          //‘N1’ generates secret question CRPK on dynamically generated input and send it to ‘N2’.
$N1 \rightarrow N2 : <Challenge, M1>$
$(M2)_H = SHA1(CRPK)$     // ‘N1’ computes answer for the same question using hash function.
$(M3)_H = SHA1(CRPK)$     // ‘N2’ computes answer for the same question using hash function.
$N1 \leftarrow N2 : <Response, M3>$   //‘N1’ receives answer from ‘N2’
if $(M2)_H = (M3)_H$ then
    $N1 \rightarrow * : <LN>$      // declare N2 as is legitimate node and broadcast LN to all legitimate nodes in MANET
else
    $N1 \rightarrow * : <MN>$      // ‘N1’ declare ‘N2’ as malicious node and broadcast MN to all legitimate nodes in MANET.
end if
All nodes store this information in their MNT
Set $(RTStatus(N2) = 0)$
```

4.1 Basics of GNY Logic

GNY logic [17] is one of the logic-based approaches which is used for proving correctness of the cryptographic algorithms. Normally in GNY logic the correctness of a protocol is proven by inferring the desired end states using the assumptions, inference rules provided by GNY logic and communication steps used in the protocol. If the assumptions and inference rules are not properly applicable on any communication step in the protocol, then the protocol will fail. That is, the proofs that do not depend on all knowledge preconditions assumptions indicate that the protocol is incorrect. A protocol in the GNY logic is an ordered series of messages such as $N2 \rightarrow N1 : N1 \lhd *X$, states that N2 send a message X to N1 that is a message *X is being told to N1 by N2. ‘*’ indicates not-originated-here mark. Then based on inference rules provided by GNY Logic [17] and assumptions made for the protocol, the messages can be verified as described later in section 4.2.

4.2 OTNA Protocol Correctness Proof

In this section, GNY logic [17, 18] is used to prove OTNA protocol's correctness. The OTNA protocol is based on cryptographic one way hash function. The outcome of OTNA protocol is depending on knowledge preconditions of nodes: if one of the nodes does not know the Node Authentication Unit (NAU) before the protocol run, that node will not learn NAU during protocol run. The protocol described in previous section 3 has two participating principal nodes, N1 legitimate node (verifier) and N2 New node (Prover). Following steps describes GNY logic for OTNA protocols correctness.

1. Specify the Idealized Protocol Messages

The idealized protocol is described in previous section 3. The messages that are exchanged during OTNA protocol run is written in the "language" of the GNY logic as follows:

1. N2 → N1 : N1 ⊲ *{*RREQ, *N2}, N1 ⊲ *{*RT(status), *MNT, *C}
2. N1 → NextHop : NextHop ⊲ *{*RREQ, *N1}
3. N1 → N2 : N2 ⊲ *{*CRPK, *S},
4. N2 → N1 : N1 ⊲ *{*H(CRPK), *S, *N2}
5. N1 → All : All ⊲ *{N2}

2. Notations and Assumptions

Notations

RT(status): Status field of Routing Table that describes Authentication status of the node.

MNT: Malicious Node Table to keep information about malicious node detected during node authentication process.

CRPK: Dynamically generated message.

C: Condition for RT(status) field.

S: Secret about CRPK.

ALL: All legitimate nodes in MANET.

Assumptions

A.1 N1 ∋ N2, denotes that N1 possesses N2.

A.2 N1 ∋ RREQ, denotes that N1 Possesses RREQ.

A.3 N1 ∋ C, denotes that N1 Possesses condition (RT(status)== 0 or 1).

A.4 N1 ∋ RT(status), denotes that N1 Possesses RT(status).

A.5 N1 ∋ MNT, denotes that N1 Possesses MNT.

A.6 N1 ∋ CRPK, denotes that N1 Possesses CRPK.

A.7 N1 |≡ #(CRPK), denotes that N1 believes freshness of CRPK.

A.8 N1 |≡ Φ(CRPK), denotes that N1 believes that CRPK is recognizable.

A.9 N2 ∋ CRPK, denotes that N2 Possesses CRPK.

A.10 N2 ∋ S, denotes that N2 Possesses S secret about CRPK.

A.11 $N2 |\equiv N1 \xleftrightarrow{CRPK} N2$, denotes that N1 believes that CRPK is suitable key for N2.

A.12 N2 |≡ N1|~ (CRPK), N2 believes that N1 once conveyed CRPK.

A.13 ALL ∋ N2, RT(status), MNT, denotes that ALL nodes possesses N2, RT(status), MNT.

A.14 *N*1| ≡ *N*2, denotes that N1 believes N2.

A.15 *NextHop* ∋ *RREQ*,*N*1, denotes that *NextHop* Possesses *RREQ*,*N*1.

A.16 *N*1 ∋ *H*(*CRPK*), denotes that N1 Possesses *H(CRPK).*

A.17 *N*2 ∋ *H*(*CRPK*), denotes that N1 Possesses *H(CRPK).*

A.18 N1 |≡ N2, denotes that N1 believes N2.

3. Specify Protocol Goals

The OTNA protocol satisfies following properties:

1. "Verifier N1 believes that the Prover N2 wants to prove their identity and knows secret about CRPK".
2. "Only the verifier N1 learns whether anybody knows CRPK in course of the protocol execution".
3. "Nobody learns CRPK in the course of the protocol".

4. Apply Logical Assumptions on Messages

In step 1, message exchanges during OTNA protocol execution has been described.

Fig. 4 shows the flow of message exchanges during OTNA protocol execution. Now this step describes proof for the message exchanges during OTNA protocol execution.

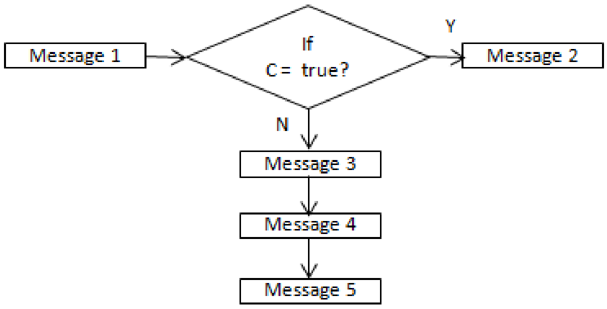

Fig. 4. Flow of Message Exchanges during OTNA protocol execution

Following are the proofs for the messages:

Message 1:
To prove message 1, N2 → N1 : N1 ⊲ *{*RREQ, *N2}, N1 ⊲ *{*RT(status), *MNT, *C}
following steps are taken:
-Apply T1, T2, P1 and P2 on message 1 to get N1 ∋ RREQ, N2, that is A.1 and A.2.
-Since N1 ∋ N2, N1 ∋ RREQ, N1 ∋ RT(status), N1 ∋ C, that is A.1, A.2 and A.3; apply P3 to get N1 ∋ {N2, RT(status), MNT, C}.
Now based on the condition C, N1 will carry on.

Message 2:
If Condition for step 1 is true, then N1 → NextHop : NextHop ⊲ *{*RREQ, *N1}, so apply T1, T2, P2 on message 2 to get NextHop ∋ RREQ, N1, that is A.15.

Message 3:
N1 → N2 : N2 ⊲ *{*CRPK, *S}
Applying T1, T2, P1, F1, R6, I6. The rule P1 shows that N2 now possesses all components, a CRPK and a secret about CRPK, that is A.9, A.10. F1 and R6 confirms that message is fresh and recognizable, that is A.7 and A.8. I6 states that N2 |≡ N1 |~ X, N2 believes that N1 sent a message, that is A.12.
Hence satisfies property 1 and 2 of the OTNA protocol.

Message 4:
$N2 |\equiv N1 \xleftrightarrow{CRPK} N2$ is valid, as per assumption A.11. Now apply T1, P4, A.9 and A.12 on message 4 to get N2 ∋ H(CRPK), S, that is A.17.
Also, at N1 side, apply T1 and P4 to get, N1 ∋ H(CRPK), S, that is A.16.
Now N1 compare H(CRPK) and based on result continue to step 5.
Hence satisfies property 1, 2 and 3 of the OTNA protocol.

Message 5:
Applying T1, T2, P1 and P2 on message 5. ALL ∋ N2, RT(status), MNT, that is A.13.

In this way, it has been proved that the OTNA protocol satisfies belief and possession properties of GNY logic, which proves the OTNA protocol's correctness.

4. CONCLUSION

Now a day's MANETs are used in variety of applications in the society. Since MANETs are ad-hoc networks, it does not use any specific infrastructure. Also, it uses multi-hop communication for packet forwarding. Due to these features of MANET, every node present in MANET must be cooperative and secure. Therefore node security plays important role in MANET. Node security can be achieved by applying authentication on every node. In existing node authentication techniques, there is no provision to keep authentication status of every authenticated node present in network. Therefore, it is necessary to perform node authentication again and again which consumes more resources. Hence, a new protocol is proposed to perform node authentication, which consumes less resources of MANET node. The protocol is named as OTNA protocol.

The OTNA protocol performs one time node authentication for each node only once whenever node enters in MANET. And the authentication status will be kept in a 'status' field of legitimate node's routing table. Therefore, only two nodes are involved to authenticate a node, which makes other nodes available for packet forwarding process. And no central authority is involved in node authentication process. In OTNA protocol, less amount of memory is required to keep information about malicious node and authentication status of a node. Also, less number of message exchanges is required to authenticate a node, which reduces control overhead during node authentication process. The OTNA protocol has been proved to be secure and correct using the GNY logic.

5. REFERENCES

[1] P. Singh, M. Chandra Pandey, "Evaluation of certificate-based authentication in Mobile Ad-hoc networks", International Conference on Recent Trends in Engineering and Technology, 2012.

[2] J. Sen, "Robust and Efficient Node Authentication Protocol for Mobile Ad Hoc Networks", Second International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM), 2010, pp. 476-481.

[3] MM Swift, B Shah, 2002. Challenge-response authentication and key exchange for a connectionless security protocol. US Patent. Google Patents, 2002.

[4] D. Djenouri, N. Badache, "Survey on security issues in Mobile Ad-hoc Networks", IEEE communications surveys, 2005.

[5] N. Komninos, D. Vergados, C. Douligeris, "A Two-Step Authentication Framework in Mobile Ad-Hoc Networks", China Communication Journal, 2007.

[6] H deng, A. Mukharjee, D. Agrawal, "Threshold and identity-based key management and authentication for wireless network", International conference on Information technology: coding and computing (ITCC'04), Vol. 1, 2004.

[7] L. Zhou, Z. Haas. 1999. Securing ad hoc networks, IEEE Network Journal, Vol 13, no. 6, 1999, pp 24-30.

[8] J. Kong, P. Zefros, H. Luo, S. Lu, L. Zhang, "Robust and ubiquitous security support for mobile ad hoc networks" in Proceedings of the 9th International Conference on Network Protocols, 2001, pp 251-260.

[9] G. Montenegro, C. Castellucia, "Statistically unique and cryptographically verifiable (SUCV) identifiers and addresses", in Proceedings of the Network and Distributed System Security Symposium, 2002.

[10] L. Eshenauer, V.D. Gligor, J. Baras, "On trust establishment in mobile ad hoc networks", in Proceedings of the Security Protocols Workshop, LNCS vol no 2845,Springer- Verlag, 2002.

[11] A. Abdul-Rahman, S. Hailes, "A distributed trust model", in Proceedings of the New Security Paradigms Workshop, Langdale, Cumbria, United Kingdom, 1997, pp. 48 - 60 .

[12] J. S. Baras, T. Jiang, "Managing trust in self-organized mobile ad hoc networks", in Proceedings of the 12th Annual network and Distributed System Security Symposium(NDSS 2005), Wireless and Mobile Security Workshop, February 2005, San Diego, California, USA.

[13] J. Sen, P. R. Chowdhury, I. Sengupta, "A distributed trust establishment scheme for mobile ad hoc networks", in Proceedings of the International Conference on Computing: Theory and Applications, 2007, pp. 51-58 .

[14] J. Sen, A. Ukil, D. Bera, A. Pal, "A distributed intrusion detection system for mobile ad hoc networks",in Proceedings of the 16th IEEE International Conference on Networking(ICON 2008), New Delhi, December 2008, pp. 1-6.

[15] M. K. Rafsanjani, A. Movaghar, "Identifying Monitoring Nodes with Selection of Authorized Nodes in Mobile Ad Hoc Networks",World Applied Sciences Journal, vol. 4, no.3, 2008, pp. 444 – 449.

[16] M. Burrows, M. Abadi, R. M. Needham, "A Logic of Authentication". ACM Transactions on Computer Systems, Vol. 8, No. 1, Feb 1990, pp. 18-36.

[17] L. Gong, R. Needham, R. Yahalom, "Reasoning About Belief in Cryptographic Protocols". In proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, Oakland, 7-9 May 1990.

[18] W. Teepe, "Proving Possession Of Arbitrary Secrets While Not Giving Them Away:New Protocols And A Proof In Gny Logic", Synthese, 149(2), March 2006, pp.409–443.

[19] A. D. Rubin, P. Honeyman, "Formal Methods for the Analysis of Authentication Protocols", CITI Technical Report. *Technical Report CITI* TR, October 1993.

[20] K. Naik (Joshi), A. Dixit, "Resource Aware Node Authentication Framework for Secure MANET", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16,May-Jun.2014,pp.109-113.