Journal of Computer Science 10 (12): 2488-2493, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.2488.2493 Published Online 10 (12) 2014 (http://www.thescipub.com/jcs.toc)

SECURE WIRELESS AD HOC NETWORKS USING ZERO KNOWLEDGE PROOF

[1]Benfano Soewito, [2]Yonathan Marcellinus and [3]Manik Hapsara

[1,2]Graduate Program in Informatics, Bina Nusantara University, Jakarta, Indonesia
[3]Master Program in Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia

Received 2014-08-08; Revised 2014-09-17; Accepted 2014-12-26

ABSTRACT

A Mobile Ad-hoc Network (MANET) is a group of wireless mobile nodes that dynamically form a network without any pre-established infrastructure or centralized administration, Soewito (2014). Some network hops may be needed to send a packet from one node to another node in the MANET. To do the communication between the nodes, a route has to be selected in the network, therefore it need a routing protocol that manage selection of the route. Selection route in mobile ad-hoc network is not easy because nodes always move so that the topology of network always changed every time. This is a big issue in selection route in mobile ad-hoc network because the route can be broken anytime. Moreover, MANET is more vulnerable than other wireless communication types because every mobile node serves as both the host and the router and forwards packets on behalf of each other. This study presents the analyzing and evaluation several routing algorithms and a novel scheme to build an authentication system by adding the modified zero knowledge proof algorithm to each mobile node in MANET.

Keywords: Wireless Network, Ad Hoc Network, Zero Knowledge Proof, Security

1. INTRODUCTION

The mobile ad hoc network consists of wireless devices that can communicate each other. These wireless devices called mobile nodes. Soewito (2014) said that a mobile node can be a computer, printer, Global Positioning System (GPS), Personal Digital Assistant (PDA), smart phone, tab, a vehicle with mobile terminals, or any other devices capable of sending and/or receiving data generated by other mobile nodes on the network. Nodes in MANET always move around, that's mean the nodes have high mobility. The mobility of the nodes can cause the network topology to change very fast and resulting in highly unpredictable routes between one node to others nodes. The selecting of route in mobile ad-hoc network is a main issue because the routing are not reliable and may broken at anytime as stated by several authors (Soewito, 2014; Patil and Sahoo, 2013; Bekmezci *et al*., 2013).

Applications of ad-hoc networks include sensor networks, commercial and educational use, emergency cases and military communication as stated by Soewito (2014; Kiess and Mauve, 2007). For example, we are faced with a situation that a serious disaster has occurred in a particular region. In this situation, it was found that all means of communications in the area of disaster such as the internet or mobile phones are completely down. To help the people in that area then ambulance service, fire service, the national Self-Defense Forces and police will rush come to the disaster site. Every vehicle that they arrive equipped with mobile terminals that form part of an ad-hoc network. Every member of staff also has a mobile terminal in hand. In this situation, all personnel can construct an ad-hoc network by using communication tools that they are carrying, so that they can communicate and send data even the internet is down.

Mobile ad hoc network is more vulnerable than other wireless communication even though MANET has many advantages over other wireless communication. This vulnerability is caused by mobile nodes can be a hosts or routers and also it can forwarding packets between one

Corresponding Author: Benfano Soewito, Graduate Program in Informatics, Bina Nusantara University, Jakarta, Indonesia

node to another nodes. More over the routing protocols published for ad hoc network unfortunately do not have the security in their design. The most important in security wireless ad hoc network is how trust the data received by a node is sent by the authorize node. In this research we analyzed several famous routing protocols in ad-hoc network and we also introduced the modified zero knowledge proof algorithm to build an authentication system in wireless ad hoc network. Zero knowledge proof introduced and published by Jacques *et al*. (1989) reported that in a paper entitled "How to Explain Zero-Knowledge Protocols to Your Children". Recently, the concept of zero knowledge proof became very popular and widely used in cryptographic systems. In this concept, there are two parties involved, namely prover and verifier. With this technique allows a prover shows that he has the right or evidence (credential) without have to show the actual values to the verifier. The concept of zero knowledge proof will be discussed in section 3 in detail.

This study is structured as follow: In section 2 discussed about ad hoc routing protocols and describes the method to find the route and the route maintenance. Section 3 describes the concept of zero knowledge proof of discrete logarithms. Section 4 describes the methodology of the research and the steps to simulate of the wireless ad hoc network and modified zero knowledge proof. Section 5 describes the result of our experimental and section 6 concludes of our research.

2. WIRELESS AD-HOC ROUTING PROTOCOLS

Soewito (2014) found that Ad Hoc routing protocols can basically be divided into three classifications: Proactive (table-driven), on-demand (reactive), or hybrid (a combination of the previous two).

2.1. Proactive Routing Protocols

Each node in the proactive routing protocols must have information on the route to all nodes and all the time the information is always updated. Soewito (2014) stated that hese protocols require each node to maintain one or more tables to store routing information and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. Out of date information in the routing table can be known by the nodes with the mark on the serial numbers. This is very important so that no routing loop will occur. The weakness of proactive routing protocols are nodes must frequently update the routing table so that the network will always be busy in adjusting the information in the routing table, whereas the nodes is always moving at all times.

2.2. On-demand Routing Protocols

The principle of on-demand routing protocols is the route will be made at the time a node will transmit information. This technique is very different from the technique of table-driven routing on proactive routing protocols. In this technique, a node wishing to send information will start with the route discovery process. Soewito (2014) stated that this process is completed once a route is found or all possible route permutations have been examined and after a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired. The weakness of on-demand routing protocols is the time required to build a route when a node wants to transmit information and often occurs after the route is established, the route becomes disconnected due to the movement of each node. Therefore the route discovery process should be repeated to find a new route.

2.3. Hybrid Routing Protocols

To reduce the weaknesses of the two routing protocols in section 2.1 and 2.2 then there is some research that combines these two techniques are called hybrid routing protocols.

Unfortunately, in mobile ad hoc network do not have standard for routing protocol yet. Soewito (2014; Sun *et al*. (2012) stated that every routing protocol in ad hoc network has disadvantage and advantage depend on the topology of network, active sources, mobility rate and traffic field. In particular scenario and conditions, a routing protocol can shows better performance compared with other routing protocols but when the network topology changes and network parameters also change, the routing protocol will not necessarily be better than the other, it can even be the most unfavorable performance.

3. ZERO KNOWLEDGE PROOF

Authentication system in wireless ad hoc network can use Zero Knowledge Proof (ZKP) algorithms because the ZKP has the unique characteristic and properties: Completeness, soundness and zero knowledge.

3.1. Completeness

If the declaration is true, authentic verifier (i.e., one following the correct protocol) will be assured of this circumstance by the honest prover.

3.2. Soundness

If the declaration is false, no fraud prover can assure the honest verifier that it is true, unless with few possibility.

3.3. Zero-knowledge

If the declaration is true, no fraud verifier absorbs anything other than this circumstance. It was unveiled by presenting that every fraud verifier has some simulator that, assumed only the declaration to be proven (and no entree to the prover), can generate a transcript that "looks like" and contact between the honest prover and the fraud verifier.

Jacques *et al*. (1989) illustrate the zero-knowledge proof by using a story about a cave that has a secret. In this illustration there are two people, Peggy (prover) and Victor (the verifier).

As shown in **Fig. 1**, every person who knows the key words or password can open a secret door between C and D. Suppose Peggy wanted to show to Victor that she knew the key word to open the secret door, then Peggy and Victor need to do is as follows:

- Victor stands at point A
- Peggy walked into the cave towards point C or D
- After Peggy is not seen in the cave, Victor goes to point B
- Victor then ordered to Peggy for:
- Walking out from the left or right side
- Peggy response and use key word that she had to open the secret door
- Peggy and Victor would then repeat these steps until *n* times

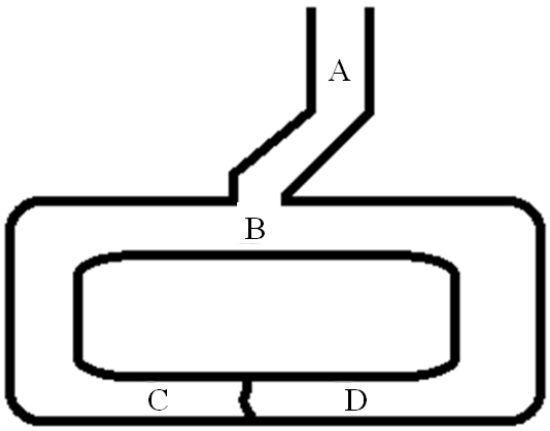

Fig. 1. A cave as an illustrate of zero knowledge proof

If Peggy has a keyword or password, then she will walk out from the side as Victor ordered to her. Probability of guessing correctly will be very little if it done repeatedly (Schneier, 1996).

In the application of Zero Knowledge Proof is done by mathematical calculations, one with the calculation of discrete logarithms. In the study Brandon (2010) discusses the techniques used for web authentication using discrete logarithms. This algorithm were reported recently Camenisch (1998), Zero Knowledge Proof of Knowledge Sigma Protocol using SPK_1 {(x): $Y = g_0^x$}. The steps of algorithm as follows:

Initialization Process
Begin
Set **G** = {n1,n2,n3,n4,..}
Set index = random(0, **G**n)
Set g0 = **G**[index]
End
Registration Process
Begin
Client Set username from user's input
Client Set password from user's input
Client Set x = hashing_function (password)
Client Set Y = g_0^x
Client Send username and Y to server
Server store username and y
End
Authentication Process
Begin
Server generate random a
Server store a and send to client
Client Set x = hashing_function (password)
Client Set Y = g_0^x
Client Set index = random(0, **G**n)
Client Set rx = **G**[index]
Client Set $T_1 = g_0^{rx}$
Client Set c = hashing_function (Y, T_1, a)
Client Set $z_x = r_x - cx$
Client send c and Z_x to server
Server set $T_1 = Y^c g_0^{zx}$
Server set c' = hashing_function (Y, T_1, a)
If c equals to c' then
    Authentication is approved
Else
    Authentication is not approved
End if

4. METHODOLOGY

The uniqueness of the ad hoc network is that the network does not supported by infrastructure that has

been built in the past but this network are built by nodes that are members of the ad hoc network in the transmission range. Therefore, the ad hoc network does not need cost to build the base station and also does not require a router and does not need all existing tools that normally available in the base station.

In the ad hoc network, nodes should be able to pass on information from other nodes. If the nodes are not able to pass the information, the route between the nodes in the network will disconnected and there is no ad hoc network will be constructed. Therefore an ad hoc network is very dependent on the ability to forwarding information of the nodes that participating in the network.

Soewito (2014) stated that Ad-hoc networks are often autonomous in the sense that they only offer connectivity between participating nodes, but no connectivity to external networks such as the Internet and also network topology that always change in ad-hoc networks is another very important parameter. Soewito (2014) also stated that the topology is subject to frequent changes, due to node mobility and changes in the surrounding environment, special considerations have to be taken when routing protocols are selected for the nodes.

Another issue in ad-hoc network is security. It is very easy to tap and change the information in ad-hoc network, because in ad-hoc network, a node can be joining the network without any authentication and authorization process. The basic security that is required in ad hoc network such as confidentiality, integrity and availability.

In this study we integrated the modified zero knowledge proof algorithm to the reactive on demand routing protocols such as Ad Hoc on Demand Distance Vector Routing (AODV) and proactive table driven routing protocols such as Destination Sequenced Distance Vector (DSDV).

We start to initialization every node in the wireless ad hoc network. In this case each node become server and also as client. Each node will generate the public key g_0 and g_1 for itself that generated by randomization of group G. Moreover each node will have the table that consist the list of neighboring nodes and public keys g_0.

Next step is registration process. Each node has to in-put the username and password. This step is only done once at the beginning wireless ad hoc network was established. Then be performed hashing on the password, x = hashing (password). The hashing value will used to calculate Y, Y = g_0x. The final step in registration process is exchange the value Y between all nodes and they will put in the table on each node.

Authentication process is the last step in a zero knowledge algorithm. As shown in **Table 1**, the value that needed in this process is g_0, password and Y. In this process the nodes who will communicate will generate random rx € G and calculate T1 = $g_0$rx, c = hash(Y, T1, a) and zx = rx-cx. Then they will exchange (c, zx) and calcu-late T1 = Yc $g_0$zx, further match the c = hash(Y, T1, a). If the value c matching with c = hash(Y, T1, a) means that authentication process was done successfully. The process can be seen in **Table 2**.

After authentication process, then communication between the nodes can be started. In this study we simulated using ns-3 network simulator (Greis, 1995; NS, 2004; Ikeda *et al*., 2011). The network simulator ns-3 is an object-oriented, discrete event-driven network simulator developed at UC Berkeley and USC ISI as part of the VINT project. NS-3 is practical tool to simulate network in small or wide area of network, including wireless networks and ad-hoc networking as well. The ns-3 network simulator has become popular to researcher in area of networking, because the ns-3 easy to use and provide many modules. In ns-3, the researcher can inject the simulation scripts or can make the scenarios of experiment. This script can be written in many programming language, but the suitable is OTcl. Normally the complicated scenario can be written in C++ code that either comes with ns-3 or is supplied by the user. Sudip *et al*. (2010) stated that the flexibility of ns-3 makes it easy to enhance the simulation environment as needed, although most common parts are already built-in, such as wired nodes, mobile nodes, links, queues, agents (protocols) and applications.

Table 1. The value in the beginning authentication process

Prover (user)	Verifier (server)
g_0	g_0
Password	Y

Table 2. The values in authentication process

User (prover)		Verifier (server)
		Generate random a
Receiving a	←	Sending a
x = hash (password)		
$Y = g_0^x$		
Generate random rx		
Calculate $T1 = g_0^{rx}$		
c = hash(Y, T1, a)		
zx = rx-cx		
Sending c, zx	→	receiving c, zx
		Calculate $T1 = Y^c g_0^{zx}$
		Matching c = hash(Y, T1, a)

Sudip *et al*. (2010) stated that most network components can be configured in detail and models for traffic patterns and errors can be applied to a simulation to increase its reality. There even exists an emulation feature, allowing the simulator to interact with a real network. Soewito (2014) stated that simulations in ns-3 can be logged to trace files, which include detailed information about packets in the simulation and allow for post-run processing with some analysis tool.

In this research we have simulated the wireless ad hoc routing protocol use AODV and DSDV. Maltz (2001; Soewito, 2014) stated that AODV is a reactive ad-hoc routing protocol and it also discovers routes on an as needed basis via a route discovery process similar to route discovery in DSR routing protocol.

However, AODV uses a slightly different technique to maintain the routing table. AODV use a conventional routing table which is one entry for each one destination. The method of maintenance table routing on the AODV is different with techniques on DSR, in the DSR multiple entries for a particular destination can be maintained with the use of cache. Soewito (2014) stated that without source routing, AODV relies on routing table entries to propagate a Route Reply (RREP) back to the source and, subsequently, to route data packets to the destination. In AODV, out of date information in the routing table can be known by the nodes with the mark on the serial numbers. All packets will have this serial number on the packet header. This is very important so that no routing loop will occur.

In the Destination Sequenced Distance Vector (DSDV), the routing table must be updated periodically and sends the routing table that has been updated to all nodes in the network. This method is called table-driven algorithm that works is similar to the Bellman-Ford routing algorithm. Soewito (2014) stated that each node in the network maintains a routing table that has entries for each of the destinations in the network and the number of hops required to reach each of them. In this technique, to prevent routing loops occurred; there is a sequence number system that created a special sequence number for each entry that is useful to know the information that is already out-of-date. Some parameters also broadcast together at the time of broadcast routing tables that has been renewed. The parameters that were broadcasted included the number of hops to the destination, the address of destination, the sequence number of the information received to the destination, as well as a new unique sequence number to be broadcasted. The selection of the route in this technique will always be based on the latest sequence number. Soewito (2014) reported that when a neighbor B of A finds out that A is no longer reachable, it advertises the route to A with an infinite metric and a sequence number one greater than the latest sequence number for the route forcing any nodes with B on the path to A, to reset their routing tables.

5. RESULTS

To simulate and evaluate the authentication system and performance routing protocols, some experiments have been done by simulation ad hoc network. Simulations were made with a focus to monitor and calculate the performance of the network with a wide variety of topologies. In simulation scenarios, we have selected the space of a certain size and in which there is a group of mobile nodes forming an ad hoc network. We simulate in two different size of the area is 500 square meters and 700 square meters. “Queue/DropTail/PriQueue” was applied as a queue system on both of method: AODV and DSDV. The average delay that was the important variable in calculating the performance of network has been recorded.

The cost to be paid after applied the zero knowledge proof on the ad hoc network shown in **Table 3 and 4**. In **Table 3**, we simulate the area of network is 500×500 meters and number of nodes is 30 nodes. After we add the zero knowledge proof algorithms, the average delay increase as much as 4.18% using the AODV routing protocol and 3.7% using the DSDV routing protocol.

In **Table 4**, we simulate the area of network is 700×700 meters and number of nodes is 30 nodes. After we add the zero knowledge proof algorithms, the average delay increase as much as 6.42% using the AODV routing protocol and 5.02% using the DSDV routing protocol.

Table 3. The percentage of overhead after applied ZKP in area of 500×500 with 30 active nodes.

	Average delay	
Mobility rate	AODV	DSDV
2	4.50	3.8
10	4.40	3.7
20	3.60	3.8
50	4.10	3.6
100	4.30	3.6
Average	4.18	3.7

Table 4. The percentage of overhead after applied ZKP in area of 700×700 with 30 active nodes

	Average delay	
Mobility rate	AODV	DSDV
2	6.70	5.60
10	5.80	4.70
20	7.40	5.50
50	6.50	4.60
100	5.70	4.70
Average	6.42	5.02

6. CONCLUSION

In this study, we discuss two aspects of mobile ad-hoc network; they are a routing and an authentication method. We presented the zero knowledge proof algorithms applied for authentication process in a wireless ad hoc network. The purposed of this study is to add security in wireless ad hoc network by applying the zero knowledge proof algorithms at the beginning wireless ad hoc network was established. We also evaluated the performance several routing protocol such as AODV and DSDV. Then we integrated the ZKP algorithm to the both of routing protocol.

Experimental result shown that the nodes were not belonging to network could not join to this wireless network. Only the nodes that have been registered can join to the MANET. This will make the network secured. In the other hand, there is some cost in applying the algorithm. The average delay will be increase between 4.18 to 6.42% for AODV routing protocol and 3.7 to 5.02% for DSDV routing protocol.

7. REFERENCES

Bekmezci, I., O.K. Sahingoz and S. Temel, 2013. Flying Ad-Hoc Networks (FANETs): A survey. Ad Hoc Netw., 11: 1254-1270. DOI: 10.1016/j.adhoc.2012.12.004

Brandon, L.J., 2010. Implementing Zero-Knowledge Authentication with Zero Knowledge (ZKA_wzk). Phyton Papers Monograph.

Camenisch, J.L., 1998. Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem.1st Edn., Hartung-Gorre-Verlag, ISBN-10: 3896492861, pp: 174.

Greis, M., 1995. Tutorial for the network simulator “ns”.

Ikeda, M., E. Kulla, L. Barolli, M. Takizawa and R. Miho, 2011. Performance evaluation of wireless mobile ad-hoc network via NS-3 simulator. Proceedings of the 14th International Conference on Network-Based Information Systems, Sept. 7-9, IEEE Xplore Press, Tirana, pp: 135-141. DOI: 10.1109/NBiS.2011.29

Jacques, J.Q., L.C. Guilou and T.B. Berson, 1989. How to explain zero-knowledge protocols to your children. Proceedings 9th Annual International Cryptology Conference, Aug. 20-24, Santa Barbara, California, USA, pp: 628-631. DOI: 10.1007/0-387-34805-0_60

Kiess, W. and M. Mauve, 2007. A survey on real-world implementations of mobile ad-hoc networks. Ad Hoc Netw., 5: 324-339. DOI: 10.1016/j.adhoc.2005.12.003

Maltz, D.A., 2001. On-demand routing in multi-hop wireless mobile ad hoc networks. MSc Thesis, Carnegie Mellon University.

NS, 2004. The network simulator: Building ns. ns-2.27.

Patil, A. and A. Sahoo, 2013. Routing protocols for ad-hoc wireless networks. Department of Electrical and Computer Engineering, Michigan State University.

Schneier, B., 1996. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2ed Edn., John Wiley and Sons, Inc, ISBN-10: 0471117099, pp: 758.

Soewito, B., 2014. Performance optimization wireless Ad Hoc networks based on routing protocols. Int. J. Control Automat., 7: 49-64. DOI: 10.14257/ijca.2014.7.2.06

Sudip, M., K. Sanjay, S. Mohammad, V. Karan and G. Pushkar, 2010. A low-overhead fault-tolerant routing algorithm for mobile ad hoc networks: A scheme and its simulation analysis. Simulat. Modell. Pract. Theory, 18: 637-649. DOI: 10.1016/j.simpat.2010.01.008

Sun, J., H. Si, Y. Wang, J. Yuan and X. Shan et al., 2012. Field architecture for traffic and mobility modelling in mobility management. Int. J. Ad Hoc Ubiquit. Comput., 10: 241-251. DOI: 10.1016/j.adhoc.2012.12.004