Research Journal of Applied Sciences, Engineering and Technology 5(10): 2946-2950, 2013
DOI:10.19026/rjaset.5.4604
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: September 15, 2012 Accepted: October 31, 2012 Published: March 25, 2013

Research Article

An Efficient Enhancement for the Security of A-SAODV Protocol

Hangzhou Li, Jianming Liu and Zhiyong Pang
School of Life and Environmental Sciences, Guilin University of Electronic Technology, Guilin Guangxi 541004, China

Abstract: This study analyzed the performance of SAODV and A-SAODV and proposed a security improvement for SAODV by introducing the concept of trust level. Further optimization has also been imposed on the current SAODV to minimize the processing overhead and delays, while maximizing the routing throughputs. NS2 simulation Results demonstrate the improved performance of our modified A-SAODV scheme.

Keywords: Reply decision, routing security, threshold, trust level

INTRODUCTION

The mobile Ad hoc network is a multi-hop, self-organize wireless network which is widely used in battlefield, conference communication and disaster evacuation .etc. But it is easily attacked because of the open transmission medium and the mode of self-organization. In addition, many security routing protocols designed for ad hoc network are too complex to implement. Hence, it's important to design a high efficient and secure routing protocol which can work autonomously under unmanned operation circumstance in ad hoc networks (David and Alessandro, 2008; Deng-Yin and Jun-Ling, 2010; Liang-Long *et al*., 2009).

Traditional security routing protocols, such as SAODV, SRP, SEAD, ARAN and SAR, resist attacks by authentication and encryption in link layer, multi-path routing and duplex identity authentication. These protocols have been trying to optimize the performance on security, extensibility, robustness and communication complexity and calculation burden. However it is still an open problem to tradeoff between security and efficiency. In this study, we focused on the popular SAODV, aiming to optimize its security efficiency.

SAODV is a security routing protocol with high efficiency, which originates from AODV protocol. The security measures, such as digital signature, authentication and hash chain, win enhance the security while increasing the computation burden and time delay, which deteriorates the protocol performance. We therefore have to improve SAODV for better protocol performance.

Many researchers have proposed improvement schemes on SAODV. It was shown in Liang-Long (2009) that they studied some evaluation and performance comparisons of AODV, SAODV and A-SAODV routing protocols, based on the performance metrics rather than security metrics. In the research of Manuel (2002) and Papadimitratos and Haas (2002), they proposed improvement schemes on SAODV based on adaptive mechanism namely A-SAODV.

This study compares SAODV protocol with A-SAODV protocol and proposed an improved scheme. We introduced the concept of trust level into A-SAODV based on adaptive mechanism and optimized it furthermore, which achieved effective integration of security and efficiency.

ANALYZE THE PERFORMANCE OF SAODV

- **SAODV protocol:** SAODV protocol is based on RSA public key cryptosystems. It is an extension of AODV security architecture. Extended AODV routing message is added on safety fields. It's necessary to conduct group authentication between end node and intermediate node. SAODV protocol adopt digital signature and hash-chain not only protects route discovery and route maintenance process but also protects integrity of routing group. Digital signature is used to protect non-mutable fields in routing message. Hash-chain assures that mutable field in the message can not be maliciously modified. The design process is as follows:

Under the Consideration of RREQ and RREP from SAODV protocol, there are two strategies can guarantee the safety of routing discovery process. The first is the most basic one, where only the destination node can reply RREP. The second preserves the

Corresponding Author: Hangzhou Li, Department of Life and Environmental Sciences, Guilin University of Electronic Technology, Guilin Guangxi 541004, China

cooperation mechanism of AODV, which can reply RREP when intermediate node has the legal routing to the destination node.

Under the first strategy, source node uses its own private key to encrypt RREQ and makes signature extension carry generated digital signature. And then intermediate nodes verify the signature of RREQ using source node public key carried by RREQ and create a new reverse route arriving at the source node. When it was verified successfully, intermediate nodes store the source node certification carried by RREQ in the relevant routing table and support the routing request response subsequently. Similarly, In order to create a forward routing in destination node, intermediate node has to store destination nodes certification carried by RREP in the relevant routing table. At last, after destination node received RREQ, it encrypts the RREP replied by itself private key. On the returning way, various nodes use the same method to verify RREP.

In the second strategy, the signature process is similar to the first one. The different process is that the source node needs to generate two digital signatures for RREQ. When intermediate nodes certify the first signature, they need to store the second signature in the reverse routing to the source node. When these nodes work as the intermediate nodes to response the routing request from other nodes, they will carry stored signature in the responded RREP packet as the evidence of owning the routing to the destination node.

The protocol can protect against all kinds of external attacks efficiently. However the authentication of node has to do a great deal of calculation and the design of double signature increases the complexity of packet length and nodes. Furthermore, the protocol needs to be improved at turner attacking detection and resisting refusing service attack.

- **Optimizing the SAODV: A-SAODV:** Recently, Cerri and Ghion proposed and realized a performance optimizing of SAODV based on adaptive mechanism: A-SAODV (Adaptive-SAODV)protocol. This protocol is used for multithread application. It includes two threads; one is specialized in execution of encryption operation, which can avoid obstruction on other packet processing. Other completes all other functions, Such as routing message processing, SAODV routing table management, timeout management, SAODV packet production and packet transfer etc. These two threads communicate through a FIFO queue which stores all packets that need to signature and verification.

We noticed that AODV protocol is more efficient because intermediate node can reply RREP instead of destination node and this operation will not aggravate node's burden. It's different under the same condition in SAODV that intermediate nodes need a large number of calculating to complete signature verification course when they reply RREP instead of destination node. This certainly will aggravate nodes processing burden and cause delay and obstruction. In order to solve this problem, A-SAODV optimized double signature characteristic by using adaptive reply decision. Intermediate nodes reply RREQ according to themselves load status. When the burden of packet signature or verification production is overload, intermediate nodes will not reply RREP. The concrete implement processes of A-SAODV adaptive reply decision are as follows:

We assumed that the nodes of buffer queue storage need signature and verification of routing packet and buffer queue length can reflect current load status of nodes. In the beginning, protocol sets a queue threshold for buffer queue of nodes. The threshold can dynamically adjust according to the change of external conditions during the execution process. When intermediate nodes receive RREQ with satisfying condition to reply RREP, they will check buffer queue length. Vice versa they will continue forwarding RREQ instead of producing response.

Besides using adaptive mechanism, the protocol has been optimized in other ways. For example in order to avoid repeated treatment, we use cache storage signature to verify the latest routing packet and use key ring for key management. These optimization measures improve the performance of SAODV. However, the protocol exist deficiencies in some aspects such as avoiding routing group flooding, reducing amount of calculation and signature time.

SECURITY IMPROVEMENT METHOD OF A-SAODV

On the basis of above analysis, a method of security improvement is introduced.

- **Network setup:** In this study, an improved method is based on three setting as follows:

  - Select a smaller TTL (Time to leave) value as TTL threshold. A packet arrivals at destination node or is discarded after passing by TTL hop count.
  - On the path from source node to destination node, node M is the former jump node of node N. Trust level of nodes M about node N is defined as probability TL. The calculation formula is: TL = T_p/T_A ($0 \leq TL \leq 1$), T_p is the normal work times of node M during the monitor period of node N to node M. T_A is the total work times of node M during the monitor period of node N to node M. A suitable value is adopted as TL threshold. When the trust level of intermediate node is less than TL threshold, it will not participate in routing selection process.

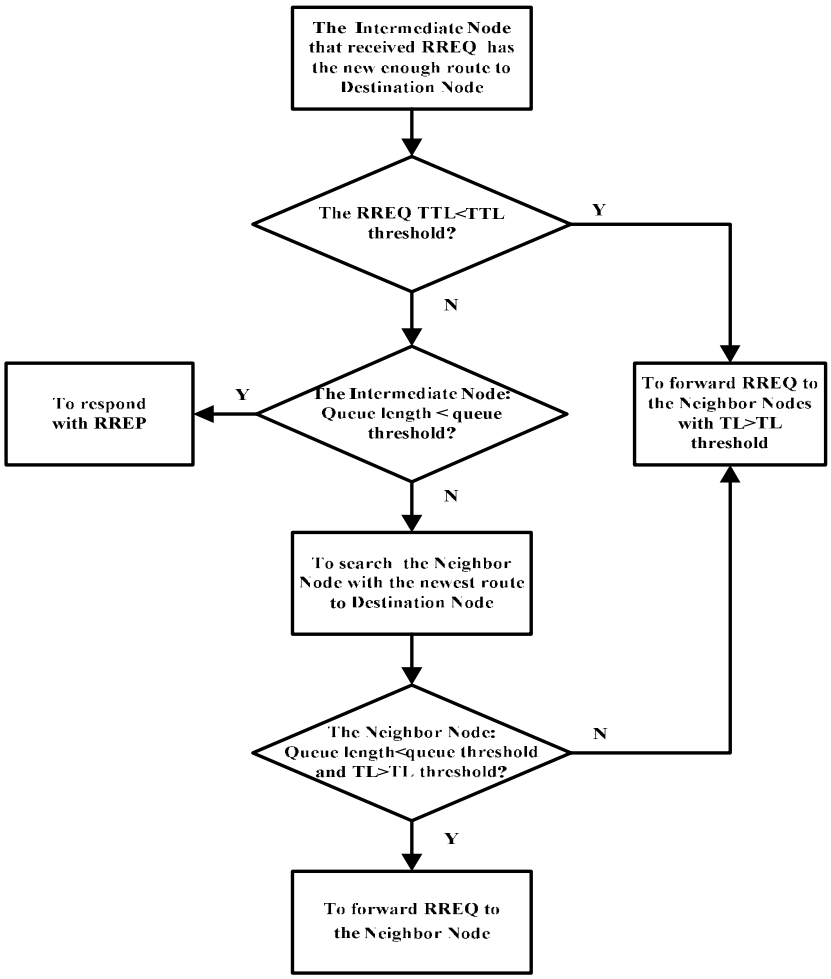

Fig. 1: Improvement scheme flowchart

- The signature extension format of routing group includes cumulative trust level field. This field is used for storing the sum of trust level of all nodes on the group path. When source node produce route finding, the cumulative trust level field of RREQ is initialized to 0. Every time before intermediate node forward RREQ, the TL value of next jump node is added to cumulative trust level field value of RREQ and then it is stored into the cumulative trust level field of RREQ. Therefore, when route finding process is finish, source node obtains multiple routing paths to destination node. The field can be used for selecting high security routes.

- **A-SAODV improvement scheme and group treatment flowchart:** According to above analysis and assumption, the concrete implement process of improvement scheme is: after receiving RREQ, if the intermediate node obtains enough new routes to destination node and satisfies with responsive condition, it will check the TTL field value of RREQ. If the field value is less than TTL threshold, intermediate node will forward RREQ to neighbor nodes which trust level is larger then TL threshold. Otherwise intermediate node will check the queue length of itself. If queue length is less than queue threshold, it will reply RREP. If routing packet signature or verification is overburdened and lead to queue length is larger than queue threshold, intermediate nodes search for next jump neighbor nodes of latest route to destination node on the routing table and check routing packet queue length and trust level of neighbor nodes. In this condition, if queue length of neighbor node is less than queue threshold and trust level is larger than TL threshold, intermediate node will forward RREQ to neighbor node, otherwise it will broadcast RREQ to neighbor nodes which trust level is larger than TL threshold. Figure 1 show the improvement scheme flowchart.

- **Load status of neighbor node and trust level in information maintenance:** In the above implementation, during the improvement of protocol, every intermediate nodes need to maintain and update the information of load status and trust level related to neighbor nodes in the routing table. It's necessary to add new queue length and trust level fields to store the information

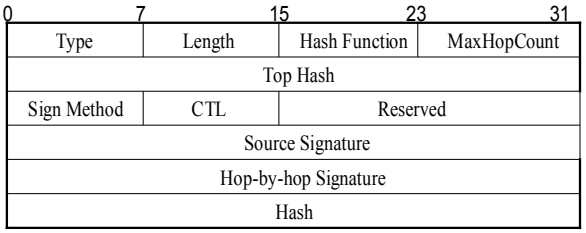

Fig. 2: The extended frame format of routing group signature

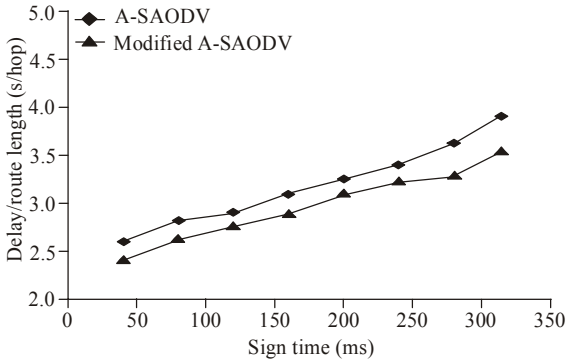

Fig. 3: Head packet delay without

in the routing table of the nodes. Furthermore, during the updating new information of load status and trust level, the time interval setup is a problem. Because if the time interval is overtime, the information of load status and trust level can't be updated on time, it leads the node to make a mistake discernment and selection. If the time interval is short, although node can obtain the latest information of load status and trust level, but information update frequently lead to large network traffic. In order to solve this problem, hello messages can carry the information of load status and trust level. Nodes realize information of load status and trust level in neighbor node updating periodically through hello messages.

- **The extended frame format of routing group signature and introduction of field:** Figure 2 shows the extended frame format of routing group signature adopted by improvement scheme, which extended frame is appended behind the routing group. Type field is the signature extended type. Its value is 32 in RREQ field, 33 in RREP field and 34 in RRER field. Length is the sum of the total length after this field, which unit is byte. Hash function field means using hash function. It's 1 when using MD5 algorithm and 2 when using SHA-1 algorithm. The value of MaxHopCount field is appointed when source node produces routing packet. The value of TopHash field is the result of hash calculation which is calculated MaxHopCount times by hash function and it is appointed by MaxHopCount field. Sign Method is a digital identification of some encryption algorithm. Its value is 1 when using RSA algorithm. It only supports this algorithm presently. CTL (accumulation trust level) field stores the sum of trust level in the node of passing on the routing group. Source Signature field stores digital signature of message from source node. The messages of signature are routing group (except HopCount region) and signature extended packet before this field. Hop-by-hop Signature stores the signature of message from intermediate node. The signature message includes routing group (except HopCount region) and signature extended packet before this field.

SIMULATION AND ANALYSIS OF RESULTS

- **Simulation setup:** Over here A-SAODV protocol is compared with the protocol that was improved by NS simulation software. When route is long, the performance of intermediate node determines the properties of the total network. Simulation environment was installed as follows for long route, so that we can give a strict test for the protocol operation efficiency: at the beginning, 100 nodes are randomly distributed in a rectangular area with boundary lengths of 1500 meter and 50 meter. The maximum connection data between nodes is 100. The maximum hostile node number is 30. The mobility model of node uses random waypoint mobility model. The fast moving speed is 20 meter per second, each pause time is 0 second and simulating experimental operates 200 seconds. All experiments use CBR stream as the data source, which transmission speed is 4 packets per second.

  The performance evaluation parameters include:

  - First data packet delay
  - Average throughput
  - Packet loss ratio

- **Study of Simulation results:** Figure 3 and 4 indicate the comparison result between improved protocol and A-SAODV protocol about head packet delay and average throughputs without hostile node attack. We can see that improved protocol is better than A-SAODV in head packet delay and average throughputs when signature time is increasing. Because improved protocol has optimized the self adaptive mechanism of A-SAODV, it reduces the burden of node, avoids flooding to a certain extent and reduces the flow of total network. Figure 5 indicates the comparison result between improved protocol and A-SAODV

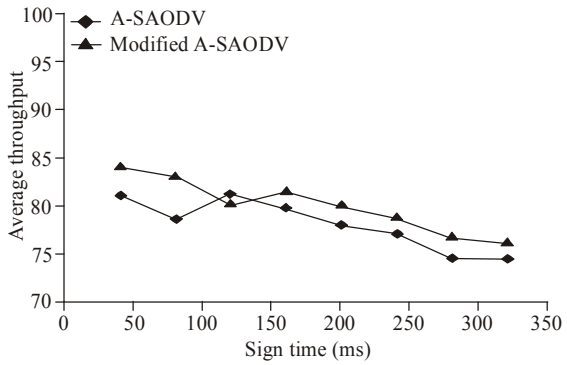

Fig. 4: Average throughputs without

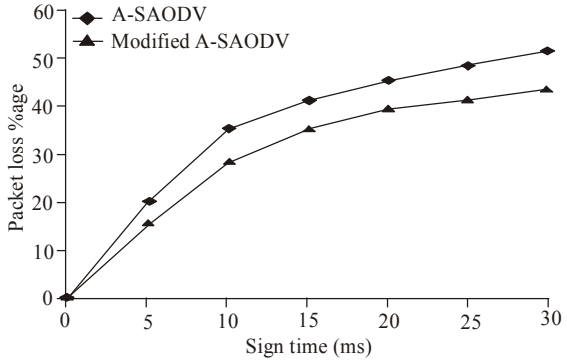

Fig. 5: Packet loss rate under hostile node attack

protocol about packet loss rate under hostile node attack. Due to introduce the security level mechanism to improved protocol, it can recognize the hostile node and reduce packet loss rate.

CONCLUSION

It's an open field at the research of AODV routing security protocol. SAODV protocol uses signature extended mode to ensure the security of route finding. But encryption calculation increases the burden of node and limits the improvement of protocol performance. A-SAODV protocol use adaptive mechanism and threshold mechanism to improve SAODV. We introduced the trust level mechanism to A-SAODV and improved adaptive mechanism of A-SAODV and obtained the balance between security and efficiency. Simulation result shows that our improved scheme can shorten the delay of End-to-End, increase throughputs and enhance the security of A-SAODV protocol. Therefore, the robustness of AODV routing security protocol is not only depending on the robustness of security mechanism but also depending on the measurement of route performance.

ACKNOWLEDGMENT

The study has been sponsored by the National Natural Science Foundation of China(61162008), Foundation of Department of Education of Guangxi Province, China (201204LX112), Foundation of Department of Education of Guangxi Province, China(201101ZD006), Open Project of Key Laboratory of Trusted Soft water of Guangxi Province, China(kx201101), Subsidy Scheme of talents of university of Guangxi Province, China(201065), Innovation Projects of Graduate Education of Guangxi Province, China(2010105950812M25).

REFERENCES

David, C. and G. Alessandro, 2008. Securing AODV: The A-SAODV secure routing prototype. IEEE Commun. Mag., 2: 120-125.

Deng-Yin, Z. and W. Jun-Ling, 2010. Research on performance comparison among improved AODV routing protocols. Comput. Tech. Dev., 20(1).

Liang-Long, L. and D. Rong-Sheng, X. Xu-Liang and W. Zhao, 2009. A secure routing protocol based on auction m mechanism for prevention of DOS attack in wireless sensor networks. Comput. Simul., 26(10).

Manuel, G.Z., 2002. Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Comput. Commun. Rev., 6(3): 106-107.

Papadimitratos, P. and Z. Haas, 2002. Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX.