Journal of Computer Science 9 (9): 1211-1216, 2013
ISSN: 1549-3636

doi:10.3844/jcssp.2013.1211.1216 Published Online 9 (9) 2013 (http://www.thescipub.com/jcs.toc)

SECURING MOBILE ANT AGENT USING CHINESE REMAINDER THEOREM

[1]Srinath Doss and [2]Janet Jeyaraj

[1]Depterment of CSE, St. Peters University, Chennai, India
[2]Depterment of CSE, Dr.MGR University, Chennai, India

Received 2013-04-13, Revised 2013-07-24; Accepted 2013-07-25

ABSTRACT

Recent days, research in wireless network becomes major area for the past few decades. In wireless routing many routing methods such as table driven, source driven; many characteristics such as reactive routing, proactive routing; many routing algorithms such as dijikstra’s shortest path, distributed bell-man ford algorithm are proposed in the literature. For effective wireless routing, the recent ant colony optimization proves better result than the existing methodologies. The ant colony optimization is a swarm intelligence technique which widely used for combinatorial optimization problems such as travelling salesman, network routing, clustering. The ant colony optimization is a real time routing protocol which offers highly reliable and optimal routing for both single path and multi path routing. As the ant is a small tiny mobile agent, providing security is critical issue. In this study, a secured ant colony optimization using Chinese remainder theorem is proposed.

Keywords: Wireless Network, Secured Routing, Ant Colony Optimization, Routing Attacks

1. INTRODUCTION

The detailed survey on ACO in many engineering applications and recent developments in ACO are available in Chandramohan and Baskaran (2011a; 2012). The ants move in the network randomly at regular intervals to scan the characteristics of large number of network nodes. While moving, they collect information about the network and deliver it to the network nodes. They deliver more updated information about the network at regular interval to the every node in the network (or subnet), which speeds up the optimization process. Every node in the network can function as a source node, destination node and/or intermediate node. Every node has a routing table and the four data structures. The routing table is established in the route discovery phase and updated in the route maintenance phase based on the proposed priority and compound probability rule which uses the four data structures (Iskandarani *et al*., 2010).

Every source node in the network, in a regular interval (Δt), generates Forward Ants (FA) and the FA is circulated in the network for searching the destination. Destinations are locally selected according to the data traffic patterns generated by the local workload (Ali *et al*., 2012). Both intermediate and source nodes forward the FA in the same way. The FA carries the path source address, the destination address, the intermediate node Identification and the path information. The FA generation rate can be a function of network dynamics, data rate, time. The FA moves in the network searching for the destination using the probability routing table of intermediate nodes. The selection of the next neighbour is done randomly according to the probability distribution function. In the intermediate node, a greedy stochastic policy is applied for choosing the next hop to move.

While moving, the FA collects the information about the time length/trip time, the congestion status and the node identifier of the intermediate nodes. A sufficient number of the ants visit the neighbour corresponding to the highest probability in the routing table. However, a number of the FA have a probability to visit other nodes and other paths still have a probability to be visited. This

Corresponding Author: Srinath Doss, Depterment of CSE, St. Peters University, Chennai, India will increase the number of the FA visiting nodes in the region around the best path. In addition, it allows a fair number of FA to visit other regions in the network. Unlike flooding, a FA will be forwarded to only one neighbour (Mohan and Baskaran, 2010).

When a FA reaches its destination, the information carried by this FA path will be graded. Then, the FA will be killed and a Backward Ant (BA) will be generated in the destination. The BA carries its corresponding FA's path grade and path's intermediate nodes ID ant it will be send back to the source node by following the reverse path of its corresponding FA. As the BA moves in the reverse path, the intermediate nodes modify their four data structures based on the path grade carried by the BA and accordingly update their probability routing tables.

Finally, the source node receives the BA, updates its tables and kills the BA. FA shares the same queues as data packets, so that they experience the same traffic load. The BA takes the same path as the concern FA travelled, but in opposite direction. BA do not share the same link queues as data packets (like FA), they use the higher-priority queues reserved for routing packets, since the only task of BA is to quickly propagate to the pheromone matrices (the information accumulated by the FA). Ant System, Ant Colony System and Ant Net proposed by earlier 2004 (Chandramohan and Baskaran, 2011b) are the significant implementation of ACO. Initially, the ACo applied the simple probability rule and later it extended to the state transition rule for the decision model.

2. MATERIALS AND METHODS

2.1. Ant as a Mobile Agent

Mobile agent is an autonomous, kind of software which migrates in the network from one host to another host. The mobile agent-based programming is attractive to design, implement and maintain distributed systems. Mobile agents used for transmitting messages, distributing network resources and interacting with other mobile agents or communicating with the distributed resource systems. The task assigned by the source node of the mobile agent will move to network such as internet to perform the assigned task. The mobile agent will return to the source node after the assigned task is completed (Eswaramurthi and Mohanram, 2013).

The characteristics of the mobile agent are listed below (Chung, 2009):

- It should be able to achieve one or more goals automatically
- It should be able to clone and propagate itself
- It should be able to collaborate and communicate with other software and agents
- It has to have a scope of competence
- It should have some evolution states to record the computation status

From the above characteristics, it is ambiguous that the ants in the ant colony system can be deployed as a mobile agent (Tashtoush and ALkasassbeh, 2013). The ant is a tiny agent hence the space complexity of the proposed system is comparably low and which reduces the network traffic. There are many research issues around the mobile agents. Few important research issues and its literature are discussed further.

Mobile agent in network security has two manifolds, security through mobile agent and securing mobile agent. In the first, the mobile agent is used for providing security in computer networks. In the second, mobile agent will meet attacks which is become critical issue in the networking domain. Securing mobile agent through Elementary Object System, which offers mutual authentication between mobile hosts and its hosting platform. Generating sub-agent for privacy protection (Ahmed, 2012), free-roaming mobile agent addresses the code, data and itinerary security issues (Prem and Swamynathan, 2012) are few recent interesting research for security.

Mobile agent causes increase of data traffic, hence, many researchers proposed methodology to reduce a number of agents migration. Reducing number of migration will lead to performance degradation, therefore trade off condition to be reached. Higashino *et al.* (2012) proposed a cached method for reducing the migration. In the cached method, the mobile agent runtime environment caches the agent codes and the agent status. The cached codes and status are reusable when a mobile agent comes back again. Thus, the method enables to reduce data traffics caused by mobile agent migration at the agent runtime environment level.

The functionalities of mobile agent (Chung, 2009) are shown in **Fig. 1**. The static security policy, security certificates and its access controls are defined as static objects and dynamic objects are defined as mutable objects.

In the proposed model, the ants are defined as mobile agent which used to propagate routing packets for mobile routing and also utilized as mobile agent for predefined task such as security of wireless network (Rahman *et al*., 2013). In this study, the ant based mobile agent is used for providing authentication between mobile nodes and control centers. The security model of the proposed paper implemented the Rivest-Shameer-Adelman (RSA) based cryptosystem with Chinese Reminder Theorem (CRT).

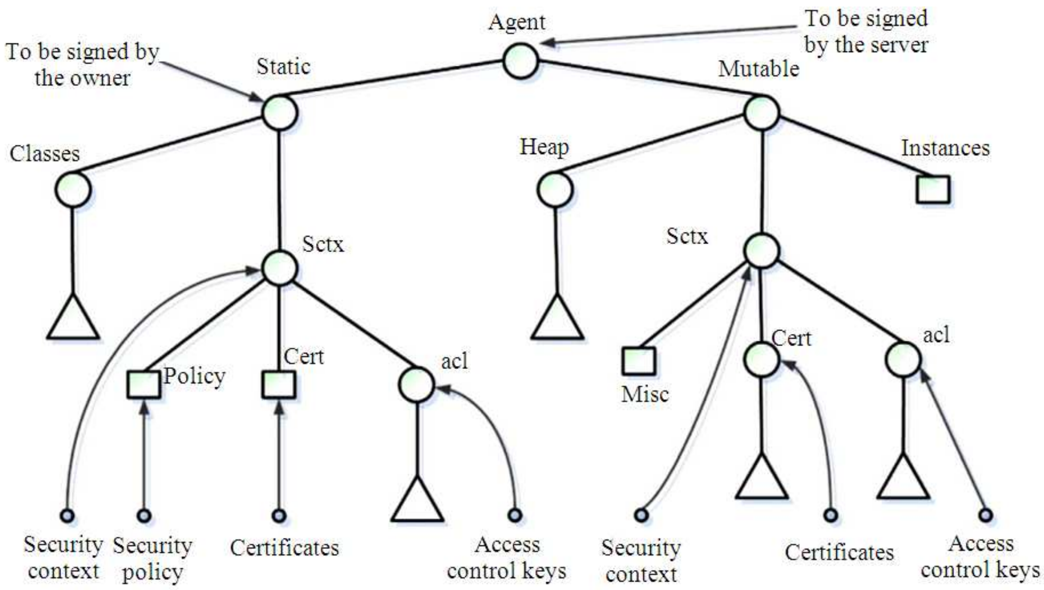

Fig. 1. Typical mobile agent

2.2. Proposed Security Model Using CRT

The proposed ant based mobile agent used for authentication using RSA-CRT cryptosystem.

The RSA is based on the assumption that factoring the product of two prime numbers. Let p and q be two distinct primes and N is computed in the following Equation 1-9:

$$N = p * q \tag{1}$$

In the RSA cryptosystem, a message m is signed with a secret key d as:

$$S = m^{d} \bmod N \tag{2}$$

e is the public key and d is the corresponding private key, so that:

$$e * d \equiv 1 \bmod \phi(N) \tag{3}$$

where, the Euler phi function of N is:

$$\phi(N) = (p-1)(q-1) \tag{4}$$

$$d_p = d \bmod (p-1) \tag{5}$$

$$d_q = d \bmod (q-1) \tag{6}$$

$$I_p = p-1 \bmod q \tag{7}$$

The Chinese Remainder Theorem (CRT) can be used to speed up the computation of the signature generation. This can achieve improvement by a factor of around four. The following Algorithm 1 shows the CRT-RSA algorithm:

```
Algorithm 1 (CRT-RSA).
Input: $m, p, q, d_q, d_p, I_p$.
Output: $S := m^{d} \bmod N$.
1: $S_p \leftarrow m^{d}_{p} \bmod p$, $S_q \leftarrow m^{d}_{q} \bmod q$.
2: $S \leftarrow CRT(S_p, S_q)$
3: Return S
```

The CRT recombination in step 2 of Algorithm 1 is usually done using the Garner algorithm. This computes:

$$S = CRT\ (S_p, S_q) \tag{8}$$

$$S = ((S_q - S_p) \cdot I_p \bmod q) \cdot p + S_p \bmod N \tag{9}$$

Let, A and B are two vectors which is defined by a rule such that the entries of A and B have only small factors. These two vectors are used to make a public vector, F with a matrix C = (cij) 2×2 by using the Chinese remainder theorem and modular multiplication in order to scramble vectors A and B. This scheme does not use a binary message. Instead of that, it uses a message $M = (m_1, \ldots, m_n)$ with $m_i \in \{0, 1, 2, \ldots, 15\}$ that is encrypted into a cipher text c such that $c = \Sigma n$. Using a non binary message, this scheme seems resistant to low-density attacks.

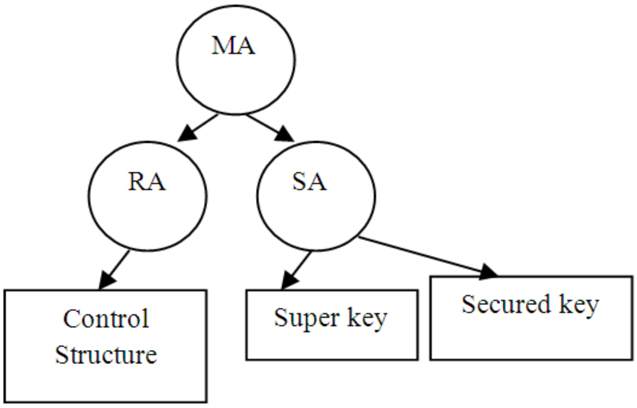

Fig. 2. The functional diagram of proposed ant mobile agent

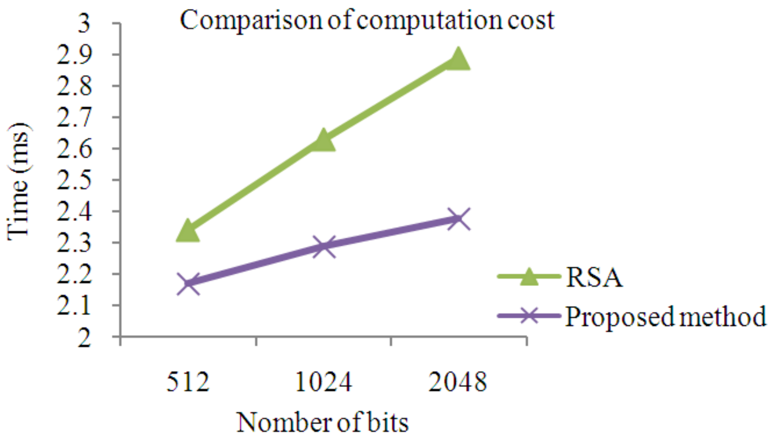

Fig. 3. Comparison of computational cost of proposed and existing methods

Table 1. Computational Cost in ms

No of Bit	RSA	Proposed method
512	2.34	2.17
1024	2.63	2.29
2048	2.71	2.38

The proposed ant based mobile agent is shown in **Fig. 2**. The proposed method has two proposed blocks, which are routing block and security block. The routing block contains the control structure for routing information collection and routing maintenance. The security model has two sub tasks which are super key and secured key. The super key is used for authentication from mobile center to all mobile nodes. The secured key is a key generated by the CRT-RSA.

The performance analysis in terms of computational cost of proposed method are computed and compared with existing RSA. The result of the same is presented in **Table 1**. **Figure 3** analyses the comparison of performance of proposed and existing method in the graphical manner.

3. RESULTS AND DISCUSSION

From the results shown in the **Table 1 and 2** which also represented in **Fig. 3 and 4**, it is identified that the computational cost and transmission cost of the proposed method are improved than the existing RSA model. The computational cost of the proposed method is reduced as a minimum of 7% to a maximum of 18%. The transmission cost of the proposed method is reduced as a minimum of 9% to a maximum of 32%, the transmission cost of the proposed work improves well when more number of flows.

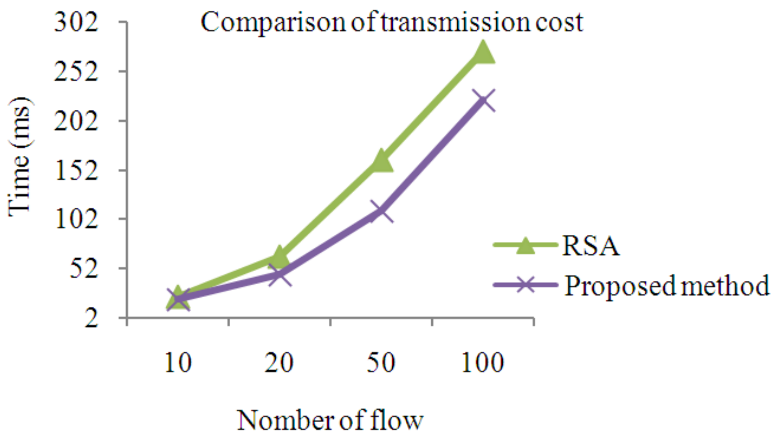

Fig. 4. Comparison of transimission cost of proposed and existing methods

Table 2. Transmission cost in Ms

No. of flows	RSA	Proposed method
10	23	21
20	64	46
50	162	110
100	272	223

Hence it is concluded that the proposed method outperforms than the existing methodologies.

4. CONCLUSION

This study proposed secured model using Ant system based mobile agent. The proposed ant mobile agent was implemented and tested on various test cases. The results are discussed in the discussion section. From the results, it is obvious that the transmission cost of the proposed system reduced around 10% and computational cost also reduced around 12%. Hence, the proposed work provides optimal result than the existing systems.

5. REFERENCES

Ahmed, T.M., 2012. Generate Sub-Agent Mechanism to protect mobile agent privacy. Proceeding of the IEEE Symposium on Computers and Informatics (ISCI), Mar. 18-20, IEEE Xplore Press, Penang, pp: 86-91. DOI: 10.1109/ISCI.2012.6222672

Ali, J., I. Ahmad, M. Faheem, M. Irfan and A.M. Gul, 2012. Factors associated with delaying of fibrinolytic therapy administration in patients with acute myocardial infarction. Khyber Med. Univ. J., 4: 129-132.

Chandramohan, B. and R. Baskaran, 2012. A Survey: Ant colony optimization based recent research and implementation on several engineering domain. Expert Syst. Appli., 39: 4618-4627. DOI: 10.1016/j.eswa.2011.09.076

Chandramohan, B. and R. Baskaran, 2011a. Reliable Barrier-free services in next generation networks. Proceedings of the 2nd International Conference on Advances in Power Electronics and Instrumentation Engineering, Apr. 21-22, Nagpur, India, pp: 79-82. DOI: 10.1007/978-3-642-20499-9_13

Chandramohan, B. and R. Baskaran, 2011b. Survey on recent research and implementation of ant colony optimization in various engineering applications. Int. J. Comput. Intell. Syst., 4: 566-582. DOI: 10.1080/18756891.2011.9727813

Chung, Y.F., 2009. Efficient migration access control for mobile agents. Comput. Standards Interfaces, 31: 1061-1068. DOI: 10.1016/j.csi.2008.09.039

Eswaramurthi, K.G. and P.V. Mohanram, 2013. Improvement of manufacturing performance measurement system and evaluation of overall resource effectiveness. Am. J. Applied Sci., 10: 131-138. DOI: 10.3844/ajassp.2013.131.138

Higashino, M., K. Takahashi, T. Kawamura and K. Sugahara, 2012. Mobile agent migration based on code caching. Proceedings of the International Conference on Advanced Information Networking and Applications Workshops, Mar. 26-29, IEEE Xplore Press, Fukuoka, pp: 651-656. DOI: 10.1109/WAINA.2012.127

Iskandarani, M.Z., 2010. A novel odor key technique for security applications using electronic nose system. Am. J. Applied Sci., 7: 1118-1122. DOI: 10.3844/ajassp.2010.1118.1122

Mohan, C. and R. Baskaran, 2010. Improving network performance using ACO based redundant link avoidance algorithm. Int. J. Comput. Sci., 7: 27-34.

Prem, M.V. and S. Swamynathan, 2012. Securing mobile agent and its platform from passive attack of malicious mobile agents. Proceedings of the International Conference on Advances in Engineering, Science and Management, Mar. 30-31, IEEE Xplore Press, Nagapattinam, Tamil Nadu, pp: 605-609.

Rahman, S.A., B.H. Lau, J. Kamaruzaman and H.N. Ramli, 2013. A working integrated model for the diffusion of construction innovation. Am. J. Applied Sci., 10: 147-158. DOI: 10.3844/ajassp.2013.147.158

Tashtoush, N.M. and O. ALkasassbeh, 2013. Determining optical constants of selenium thin films using the envelope method. Am. J. Applied Sci., 10: 164-171. DOI: 10.3844/ajassp.2013.164.171