ACO BASED MOBILE AGENT FOR SECURED KEY MANAGEMENT IN MANET

D. Srinath, V. Subedha and S. Venkatraman
Department of Computer Science and Engineering, Panimalar Institute of Technology, India
E-Mail: srinathdoss@yahoo.com

ABSTRACT

Nowadays, Wireless network becomes unavoidable resource in the modern world. Security of wireless network becomes very important critical research issue in this decade. This paper focused on various kinds of attacks and proposed methodology for authentication. Attacks which may be passive attacks or active attacks will collapse the entire operation of the whole network. The attacks on wireless network are much complicated than traditional wired network. Hence, designing a secured authentication attracts many researchers. In this paper, an ant colony optimization is proposed for mobile agent and which is used for secure group management. The ant colony optimization is a swarm intelligence based real time routing protocol which offers highly reliable and optimal routing for both single path and multi path routing. Hence, securing ant colony optimization for wireless network will lead to appreciable result.

Keyword: mobile agent, authentication, wireless network, handshake**.**

1. INTRODUCTION

In this scientific world optimization problem is of high importance [3]. Ant Colony Optimization (ACO) is a meta heuristic approach where ACO routing algorithms take inspiration from the behavior of ants in nature and from the related field of ACO to solve the problem of routing in communication networks [1] [2].This algorithm utilizes the behaviour of the real ants while searching for the food. It has been observed that the ants deposit a certain amount of pheromone in its path while traveling from its nest to the food [11].

In ACO, a number of artificial ants build solutions to an optimization problem and exchange information on their quality via a communication scheme that is reminiscent of the one adopted by real ants [4], [5]. Shortest path is identified by pheromone deposited by moving ant on the ground, so an ant encountering a previously trail can detect it and decide with high probability to follow it. ACO algorithms has a set of characterizing features that always be specified, preferably, when describing the algorithm. The construction of a solution, along with its representation, is one major issue of an ant algorithm, as it is with any other heuristic method, since it will influence the rest of the procedures to be defined. Thus, it plays a crucial role on the success of the algorithm.

Besides, it is common knowledge that it has a great effect on the running time of the ACO algorithm [13]. While mobile ad hoc networks can be quickly and inexpensively setup as needed, security is a critical issue compared to wired or other wireless counterparts. Many passive and active

Security attacks could be launched from the outside by malicious hosts or from the inside by compromised hosts [14], [15].

Key management is a basic part of any secure communication. Zhou and Hass propose a secure key management scheme by using threshold cryptography. The system can tolerate t°1compromised servers. Where this system doesn't describe how a node can contact t servers securely and efficiently in case the servers are scattered in the whole area. A share refreshing scheme is proposed to counter mobile adversaries. However, efficient and secure distributions of secret shares are not addressed [16].

Recently, many researchers study the meta-heuristics which can find the sub-optimal solution at short time. In these meta-heuristics, it is reported that Ant Colony Optimization (ACO) [9], which is inspired by feeding behavior of ants, shows the better capability than Genetic Algorithm (GA) and Simulated Annealing (SA) [12] when it is applied to Traveling Salesman Problem (TSP). The classification and different kinds of IDS are shown in Figure-1.

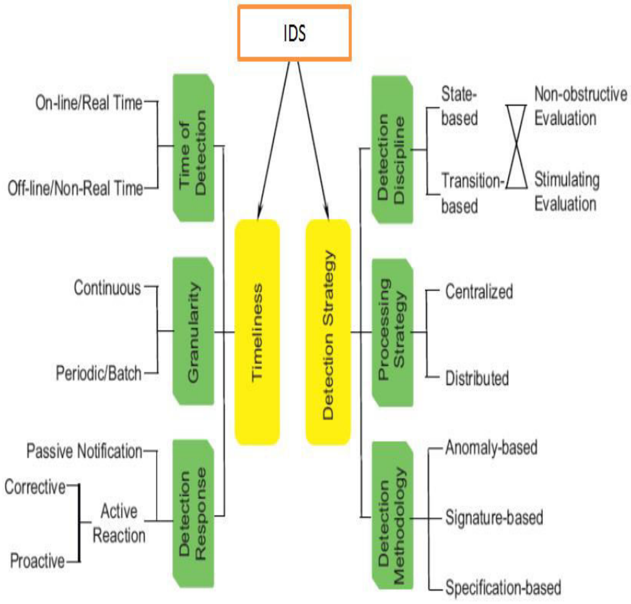

Figure-1. Kinds of IDS.

2. MATERIALS AND METHODS

The task of routing is particularly hard in Mobile Adhoc Networks. Due to the dynamic and ad hoc nature of these networks, the topology can change continuously, and paths between sources and destinations that were initially efficient can quickly become inefficient or even infeasible. This means that routing information should be updated more regularly than in traditional wired telecommunication networks [4]. However, this can be a problem in MANETs, because they typically have limited bandwidth and node resources, and make use of possibly unreliable wireless communication channels. New routing algorithms are therefore needed, which can give adaptivity in an efficient and robust way. Several researches have been carried out on routing in MANETs in recent years [10].

Existing MANET routing algorithms can be classified as being proactive, reactive or hybrid [7]. Proactive algorithms try to maintain up-to-date routes between all pairs of nodes in the network at all times. The advantage is that routing information is always readily available when data need to be sent, and the disadvantage is that the algorithm needs to keep track of all dynamic topology changes, which can become difficult when there are a lot of nodes or when they are very mobile. Examples of proactive algorithms are Destination-Sequence Distance-Vector routing (DSDV) and Optimized Link State Routing (OLSR).

Reactive (on-demand) routing protocols attempt to reduce the amount of control overhead disseminated in the network by determining routes to a destination only when it is required [6], [9]. Reactive routing algorithms only maintain routing information: they set up routes on demand. This approach is generally more efficient, but can lead to higher delays as routing information is often not immediately available when needed. Examples of reactive routing algorithms include Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance-Vector routing (AODV)[8]. In order to achieve high scalability Hybrid routing protocols such as the Zone Routing Protocol (ZRP) [17] and SHARP [18] used. It combines both reactive and proactive routing characteristics with limited region. These regions can be a cluster, a tree or a zone, which may contain a number of end-user nodes. One of the important parts of secure communication is Key management. Most of the crypto-system depends on the robust, secure and efficient key management system. Some of the key management primitives include secrecy of key, key distribution, key confidentiality, integrity and ownership. For example SRP, SEAD, and SAODV address security attacks in routing protocols and propose different means to counter particular threats. However, almost all of them rely on the existence of a public key management system. TESLA [19], delivery and authentication of the first element in hash chain requires the asymmetric key management framework.

a) Proposed work

The methodology and the security requirements of proposed Request based IDS are discussed in this section. For this extended IDS, ACO is used as Identification Agent (IA) and Target Agent (TA). In the initialization of network phase, ACO flooded in the network as IA to identify all authenticated members in order to process handshake. In the later stage, the ACO is used as TA for authenticating member and preventing non member.

Hence, there are four components in the proposed system:

- Member: Members are system belongs to a group. U ∈ G, U belongs to the group G.
- Non-member: A system does not belong to the group. U ∉ G U does not belong to the group G.
- ACO-IA used to add member to a group.
- ACO-TA used to reveal users and checking user belong to own group.

The implementation of this attractive scenario is explained hereunder:

i. **Setup:** Given a security parameter k, Setup outputs the public parameters (param) that are common to all groups.

ii. **KeyGen:** Used to generate public/secret key. KeyGen is run by ACO-IA and ACO-TA. Given param, KeyGen outputs agroup public key gpk, a secret key of ACO-IAisk and a secret key of ACO-TAtsk.

iii. **Add:** Used to add member to the group. Add is executed by a non-member A and ACO-IA. Given param, gpk and isk, Add outputs a membership certificate (certA), a secret key (skA), and ID of A (IDA).

iv. **Handshake:** It is an authentication protocol executed between two players A and B, based on the public input param. The group public keys (gpkA and gpkB), certificates (certA, certB) and secret keys (skA, skB) of A and B are input to Handshake. The output of the algorithm is either rej or acc. A Handshake ←→ B means the situation in which A and B executes Handshake.

v. **Group trace:** Given gpk, tsk and a transcript TA, B, Group Trace outputs yes if A, B ∈ G; otherwise, Group Trace outputs no. It is used for group trace.

vi. **Request reveal:** Given gpk, tsk, certA, skA, a transcript TA, B and internal information that are used in Handshake by a player A, Request Reveal outputs the member B.

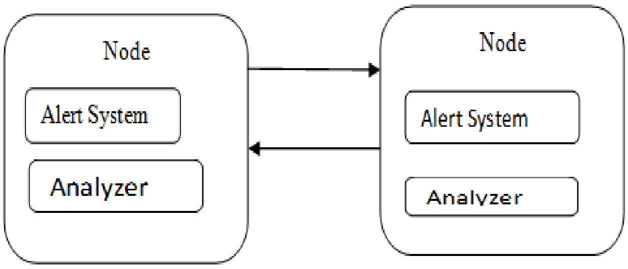

Figure-2. System design of proposed mobile agent model.

b) Security definition

The proposed mobile agent based secured model is shown in Figure-2. In each node, two types of systems are defined, such that Alert system and analyzer. The analyzer consists of mobile agent which is defined and used as program model to collect information regarding security information. The analyzer receives the security key and verifies the authentication. The alert system broadcast the alert messages to the authenticated neighbors when it identifies the intruder. This alert message also used for verification if the identified attacker may be authenticated user of other authenticated nodes of the concern node.

When an authenticated node of a group receives the message from unknown node, it initiates the mobile agent to collect security information of the unknown node. The Message Digest 5 hash function h=H(M) generates hash value, which is used to create message digest authenticated node. The authenticated node generates the following digital signature, if the unknown node is an authenticated node of the group.

$$d_{sign} = (H(M))^{d} \bmod n \quad (1)$$

The authenticated node will encrypt message by using its digital signature. Encrypting the message digest H(M) with its private key d where, n = p ∗ q, p and q are random prime numbers with p ≠ q. The source node forwards d_{sign} with data M, (d_{sign}, M) to its neighboring node through the path it takes to reach sink.

A neighboring node on reception of (d_{sign}, M) and the path in the data packet, verifies the digital signature by comparing decrypted value of d^{e}_{sign} mod n with message digest H(M). The d^{e}_{sign} mod n is key (e, n) using the formula, decrypted using sender's public

$$d^{e}_{sign} \bmod n = ((H(M))^{d} \bmod n)^{e} \bmod n \quad (2)$$

$$= (H(M))^{ea} \bmod n \quad (3)$$

By applying Little Fermat's Theorem to above Equation, it can be shown that

$$d^{e}_{sign} \bmod n = H(M) \quad (4)$$

If the generated H(M) by the receiver and the decrypted H(M) of digital signature d^{sign} is equal, then the receiver accepts the data; otherwise rejects the data and informs the sender that the data is altered through by generating route error packet. This process is repeated in every hop of the noded is joint path between source and destination. The proposed public key crypto system provides authentication, integrity and non-repudiation in the ad hoc network.

3. RESULTS AND DISCUSSIONS

The proposed work is simulated in NS2. The simulation parameters of the proposed work are shown in the following Table. The proposed work is compared with existing traditional Target Authority (TA) Model and Mobile Agent (MA) model. The Reliability and scalability are major research issues in the design of networking protocol. Hence, the proposed work are analyzed the reliability and scalability of proposed work and compared with TA and MA. The reliability is computed based on the simulation data and result. The number of node is varied and number of attacker node also varied for performance comparison.

Table-1. Simulation parameters.

Parameters	Values
Simulation area	200 × 200 m2
Propagation	Two ray ground
MAC type	802.11
Antenna	Omni antenna
Queue	Drop Tail/Priority
Queue limit	50
No of nodes	10 to 500
Packet type	CBR
Packet size	220 bits

The reliability is computed based on effective packet delivery, which analyzed on different test cases, test case 1: when 10% of attacker node, test case 2: 20% of attacker node, and test case 3: 30% of attacker node are shown in following Figure-3.

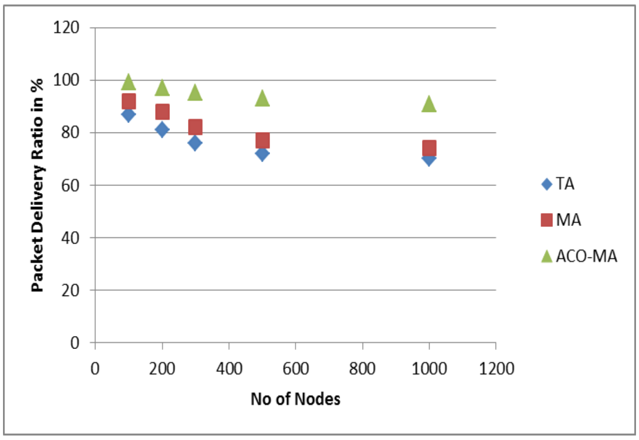

Figure-3. Reliability when 10% of Attacker Node.

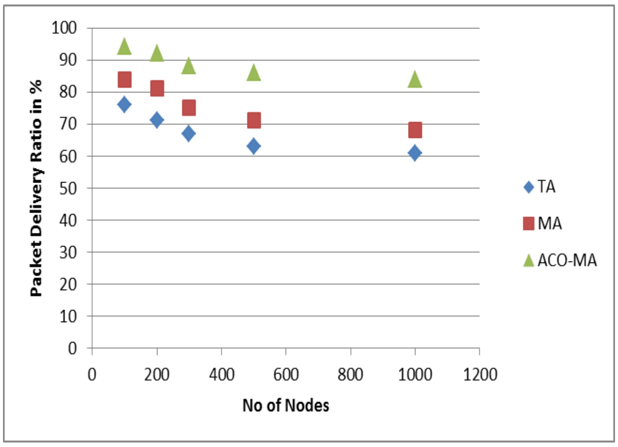

Figure-4. Reliability when 20% of Attacker Node.

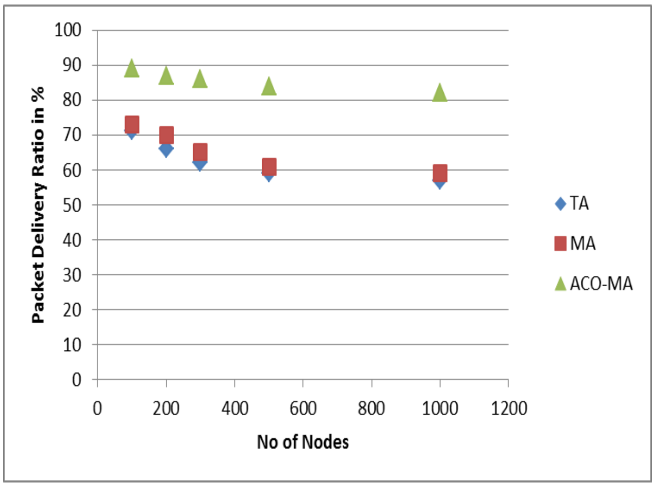

Figure-5. Reliability when 30% of Attacker Node.

4. CONCLUSIONS

The scalability is observed from the above data, in which the system has 70% and above packet delivery ratio only accepted as scalable system. Hence, when 10% attacker nodes are inserted the TA supports up to 500 Nodes, whereas MA and proposed ACO-MA support 1000 Nodes. When attacker nodes are increases, the TA supports up to 200 Nodes only, whereas MA supports 500 Nodes and proposed ACO-MA support even for 1000Nodes. Similarly, the TA and MA supports only 100 Nodes when 30% of attacker nodes are inserted. The proposed system always supports above 80% packet delivery ratio. Hence, the proposed system proves better reliability and scalability than the existing systems.

5. REFERENCES

[1] Chandramohan B. and Baskaran R. 2011. “Survey on Recent Research and Implementation of Ant Colony Optimization in Various Engineering Applications”, International Journal in Computational Intelligent Systems, Vol. 4, No. 4, pp. 566 – 582.

[2] Chandramohan B. and Baskaran R. 2012. “A Survey: Ant Colony Optimization based recent research and implementation on several engineering domain”, Expert System with Applications, Elsevier, Vol. 39, pp.4618-4627.

[3] Choochotkaew S. and Piromsopa Krerk. 2014. “An analysis of authentication models for MANETs” ISEEE International Conference on Information Science, Electronics and Electrical Engineering, Vol.3, pp.1956-1960.

[4] Feng Li and Jie Wu. 2010. “Uncertainly Modeling and Reduction in MANETs”, IEEE Transaction on Mobile Computing”, Vol.9, No.7, pp.1035-1048.

[5] Gan Rongwei, Guo Qingshun, Chang Huiyouand and Yi Yang. 2010. “Improved Ant Colony optimization algorithm for the travelling salesman problems” IEEE Journal of Systems Engineering and Electronics, Vol. 21, No.2, pp. 329-333.

[6] Hui Xu, Xianren Wu, Sadjadpour H. R. Garcia-Luna-Aceves, J. J. 2010. “A unified analysis of routing protocols in MANETs," Communications, IEEE Transactions on, Vol. 58, No.3, pp. 911-922.

[7] Krishna P.V., Saritha V., Vedha G. and Bhiwal A. 2012. “Quality-of-service-enabled ant colony-based multipath routing for mobile adhoc networks”, IET Communications, Vol.6, No.1, pp.76-83.

[8] Maity S. and Hansdah R.C. 2012. “Advanced Information Networking and Applications workshops” IEEE International Conference on Advanced Information Networking and Applications workshops. pp. 544-551.

[9] Young-Min Kim, Eun-Jung Lee and Hong-Shik Park. 2011. “Ant Colony Optimization Based Energy Saving Routing for Energy-Efficient Networks”, IEEE Communication Letters, Vol.15, No.7, pp.779-781.

[10] Srinath D. and Janet J. 2013. “Secured ant Colony optimization routing for wireless networks”, Asian Journal of Information Technology, ISSN pp. 1682-3915, Vol. 12, No. 3.

[11] M. Dorigo, V. Maniezzo and A. Colorni. 1996. "Ant System: Optimization by a Colony of Cooperating Agents", IEEE Transactions on Systems, Man, and Cybernetics–Part B, Vol. 26, No. 1, pp. 29–41.

[12] Sheibat Alhamdy, Seyed Ahmad, Noudehi, Aziz Norouzi and Majdara Mohammad. 2012. “Solving Traveling Salesman Problem (TSP) using Ants Colony (ACO) Algorithm and comparing with Tabu

Search, Simulated Annealing and Genetic Algorithm", Journal of Applied Sciences Research.

[13] Neumann F. and Witt C. 2010. Ant colony optimization and the minimum spanning tree problem. Theoretical Computer Science Vol. 411, No. 25, pp. 2406 – 2413.

[14] W. Luo and Y. Fang. 2003. A Survey of wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions. Kluwer Academic Publishers pp-319-364.

[15] I. Momhamod. 2003. Wireless networks. CRC press, 2003.

[16] Zhou, L. and Z. Haas. Securing Ad Hoc Networks. IEEE Network Magazine, Vol. 13, 1999.

[17] Z. J. Hass and R. Pearlman. 199. Zone Routing Protocol for Ad-Hoc Networks. In Internet Draft, draft-ietf -manet-zrp-02.txt, work in progress.

[18] Venugopalan Ramasubramanian, Zygmunt J. Haas, and Emin Gun Sirer. 2003. SHARP: A Hybrid Adaptive Routing Protocol for Mobile Ad Hoc Networks. In Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc), Annapolis, Maryland, June.

[19] A. Perrig, R. Canetti, J. D. Tygar and D. Song. 2000. The TESLA Broadcast Authentication Protocol. Internet Draft, Internet Engineering Task Force, July.

.