Optimizing the Generic Key Distribution Process with efficient Routing in Ad-Hoc Networks using the Ant Colony Optimization

Sharada Valiveti[1], Gaurang Raval[2]
[1]Institute of Technology, Computer Science and Engineering, Ahmedabad, Gujarat, India
[2] Institute of Technology, Computer Science and Engineering, Ahmedabad, Gujarat, India

Abstract: One of the main problems with the existing Ad Hoc network especially in the military area is the security issue. Since the network works normally in heterogeneous mode, we may have nodes belonging to some enemy forces also which may intrude the network, get the confidential information or get hold of some other nodes and change the configurations which may lead to byzantine attacks [18]. Hence security plays a very vital role in military applications. Also since there is no infrastructure specially meant for maintenance of such nodes, the nodes are supposed to be intelligent enough to do all the tasks related to network topology maintenance and security themselves. Hence Ant Colony based approach which is one of the technologies of Artificial Intelligence may be involved in such applications and we may get desirable results combining the security and routing issues together. Here in this paper, we address a very critical problem related to the network security i.e. key distribution in Ad Hoc networks using the Ant Colony Optimization in Key Distribution for Ad Hoc Networks.

Keywords: Ad hoc networks, Ant Colony Optimization, Network Security, Public Key Cryptography, Routing Protocols.

1. INTRODUCTION

The study of Security deal with the study related to possible Security Attacks, Security Services and Security Mechanisms [22]. There are different types of Security Services like Confidentiality, Authentication, Integrity, Nonrepudiation, Access Control and Availability. Depending on what security service is required, there are different types of security mechanisms provided. Security mechanisms deal with the basic methods and techniques adopted for detection and prevention of security attacks. Accordingly, identification of Security Services is crucial while designing the network. Cryptography on a whole is classified on the basis of three aspects:

- Type of operations used for transforming plaintext to ciphertext
  Substitution: Each element in plaintext is mapped into another element
  Transposition: Elements in plaintext are rearranged
- Number of Keys used
  Symmetric Key Cryptography: Single key is used for encryption and decryption
  Asymmetric Key Cryptography: Two keys are used for the entire process. One key is used for encryption while the other key is used for decryption
- The way in which plaintext is processed
  Block cipher: Processes the input one block at a time
  Stream Cipher: Processes the input elements continuously

The solution for Key Distribution addresses the second category present in the above classification i.e. number of keys used for communication. The key distribution technique mentioned here can be applicable to both, the symmetric key as well as asymmetric key distribution. Also we shall address the security services which may exploitthe usage of these keys. We here speak about the public key distribution scenario where we are transmitting the public key on need basis.

Another aspect which we have considered for the implementation of the same is the Ant colony optimization (ACO). In this topic, a brief overview of the working of basic ant as proposed by [9] is discussed. Ant movement is

DOI: 10.090592/IJCSC.2015.613

based upon a single, very simple, probability equation. While an ant has not yet completed a tour, the following equation is used to identify the next edge to take [11].

$$P = \frac{\tau(r,u)^{\alpha} * \eta(r,u)^{\beta}}{\Sigma_k \tau(r,u)^{\alpha} * \eta(r,u)^{\beta}}$$

where τ(r,u) is the intensity of pheromone on the edge between nodes r and u, τ(r,u) is a heuristic function that represents the inverse of the distance measure of the edge, α represents a weight for the pheromone, and β a weight for the heuristic. The αand β parameters define the relative importance of the two terms and how much they factor in to the probability equation. The probability is calculated for those edges only that lead to nodes not yet visited. Variable k represent the edges that have not yet been visited.

An ant tour exits when an ant has completed its visit to each of the nodes on the graph. Once the ant tour is complete, the length of the entire tour can be computed. This is simply the sum of all distances of edges traveled by the ant. The Equation shows the amount of pheromone that is left on each edge of the tour for ant k. Variable Q is constant

$$\Delta\tau_{ij}^{k}(t) = \frac{Q}{L^{k}(t)}$$

This quantity is a measure of the trail - smaller trail lengths represent higher pheromone levels while higher tour lengths represent smaller pheromone levels. The quantity is then used to increase the pheromone along each edge of the tour.

$$\tau_{ij}(t) = \tau_{ij}(t) + (\Delta\tau_{ijk}(t) * \rho)$$

This is applied to the entire path, so that each edge is provided with pheromone at a level proportional to the shortness of the path. Hence we must wait until the tour is complete before updating the pheromone levels, otherwise the actual tour length would not be known. Constant ρ is a value between 0 and 1.

On the initial tour, each edge has the same probability of being taken. In order to slowly remove edges that are part of poor paths through the network, pheromone evaporation takes place throughout all edges of the network. Using constant ρ from the above equation, we get the evaporation Equation as

$$\tau_{ij}(t) = \tau_{ij}(t) * (1 - \rho)$$

Therefore we use the inverse coefficient of the trail updates for pheromone evaporation. When the ant tour is complete, the edges updated based upon the tour lengths, and evaporation on all edges has been performed, the algorithm is restarted. The tabulist is cleared and the tour length zeroed. The ants are permitted to migrate through the network. thisprocss can be performed for a constant numebr of tours, or until no changes have been seen for some number of tours. The best path is then emitted as the solution.

This section deals with the understanding of various classifications of cryptography and the Ant Colony Optimization that is being used for key distribution. In the second section, we present the literature based on the survey done. Section III gives an insight into the understanding of the proposed architecture for key distribution. Section IV presents the implementation results and Section V presents the concluding remarks.

2. LITERATURE SURVEY

Several techniques have been implemented to perform the key distribution for both symmetric and asymmetric encryptions in Ad Hoc Networks.

Steiner1998 proposed a symmetric key distribution technique called CLIQUES [23] which was the successful distributed key agreement paradigms. It used membership events to trigger key regeneration. Keys are generated using an adaptation of well-known Diffie-Hellman Key agreement Protocol. The group controller is responsible for adding and removing members in the network.

Zhou1999 proposed the method for securing the Ad Hoc Networks which was one of the first notable publications to propose a public Key management service for ad hoc networks. The service encapsulates a public(K) private(k) key pair. The private key, k, is used to sign other nodes' public keys: the public key, K is used to verify the signature. The service employs a (n,t+ 1) threshold scheme to distribute the private key and the digital signing process among n nodes. Each of the n nodes is denoted as server node, as it has a special role in the signing process.

There are several methods suggested [22] where the key distribution is possible with the help of several handshaking signals. Here the keys are distributed on on-demand basis. Hence only if the nodes want to participate in secure communication, they exchange the keys. But the problem was that the techniques mentioned there refer to the conventional networks with some common infrastructure for key exchange like Key Distribution Centre or Authentication centre to do the needful. In case of Ad Hoc Networks it cannot be applicable because even if we may have dedicated nodes to do a particular task, these nodes are either supposed to be stationary or we may land up into unnecessary bottleneck due to centralized system for Ad Hoc Networks.

The security management in Hierarchical Ad Hoc Networks is described by Yang et.al. [25]. Here the nodes that have higher security grade can distribute the keys to other nodes that have lower security grade. When two nodes need to communicate belong to the same cluster, they need only contact the sub-servers in other cluster.

Bhargava et. al. [2][3] the authors have made use of Ad Hoc On Demand Distance Vector for routing the packets. The authors have created the intrusion detection model and intrusion response model for detection of deterministic nodes and isolation of malicious nodes respectively.

Luo2002 discuss the self securing Ad Hoc Wireless Networks [15]. An entity is trusted if any k trusted entities claim so within a certain time period.

Logical Key Hierarch (LKH) model was introduced to deal with the secure multicast and can be used for unicast also [20]. With LKH, a key distribution center maintains a key tree, which will be used for group key update and distribution. Each intermediate node in the tree represents a cryptographic symmetric key. The key distribution center associates each group member with one leaf node up to the root: the set of ksuch keys is referred to as Key Path. All users know the key at the root node. The drawback is that all ndoes have to maintain the keys from the user to the root to transmit the message to any user in the network.

Other techniques have been suggested for Key Exchange in Ad Hoc Networks as mentioned in several papers like [13] with an assumption that the public key is shared by all and using Diffie Hellman Key Exchange mechanism the key is distributed. Here ID based cryptography and threshold cryptography are used for key exchange. [16] propose the Local Tree-based Reliable Topology (LTRT) algorithm which is motivated by LMST and the Tree-based Reliable Topology (TRT).

Capkun2003 et.al proposed an approach in which public keys and certificates are represented as directed graphs. There is a directed edge from vertex Ku to vertex Kwif there is a certificate signed with private key of u that binds Kw to an identity. A certificate chain from public key Ku to public key Kvis represented by directed path from vertex Ku to vertex Kvin G. The system makes use of two certificate repositories: Updated (contains a subset of certificates that the node keeps updated) and Non-updated (expired certificates that the node does not keep updated)

[10] has proposed Adaptive Trust Evidence Distribution for Ad Hoc Networks based on Ant Colony Optimization. The trust model has two components. The first part is the trust computation model that evaluates trust level of each entity based on behavioral data or trust evidence with an assumption that the evidence that the public key of the signer is well known and authenticated, and the corresponding private key cannot be compromised.

Also the study of various papers on Cryptography with Ad Hoc Networks compromise on this part that the keys (Symmetric or Asymmetric Keys) are available to both the parties willing to communicate. This is a very big problem when communicating using Ad Hoc Networks is concerned. Hence any node which is not a part of the network, tobe configured for the network becomes a manual process but it can be handled with the help of the agents called Ants. None of these techniques use the artificial intelligence technologies for key distribution. This is the first attempt to suggest an upcoming area in Artificial Intelligence the Ant Colony Optimization for Key Distribution.

3. PROPOSED ARCHITECTURE

The Basic Ant structure as shown in Figure 1 has been derived from [14]. The requirement of each fieldof the header is as shown below:

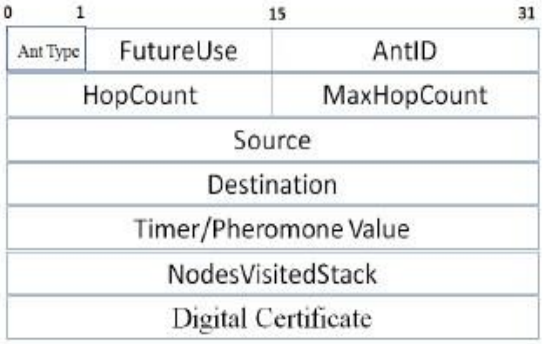

Figure 1. Basic Ant Structure in Forward as well as Backward Ants

- Ant Type: 0 if Forward Ant (Route Request Ant) and 1 if Backward Ant (Route Reply Ant)
- Future Use: Reserved for Future purpose
- Hop counts: Specifies the distance between source and destination
- MaxHopCount: Permissible maximum hop counts
- Source: Source Address
- Destination: Destination Address
- Timer/Pheromone Value: The values which specify the strength of the pheromone
- Nodes visited stack: The list of intermediate nodes
- Digital Certificate: That specifies the trust value of the node

Based on the above mentioned scheme, to take care of the problem related to Key Distribution in the Ad Hoc Network, the fields have been altered with certain value changes and a new header of the ant capable to distribute public or symmetric key is proposed as shown in Figure 2. The fields of the header are similarto what have been seen above with certain changes. They are as shown below:

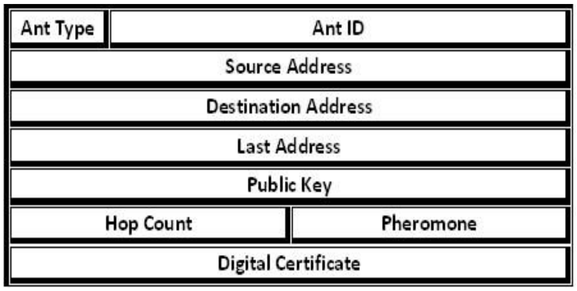

Figure 2. Proposed Ant Structure

- Ant Type: 0 if it is Forward Ant, 1 if it is Backward Ant and 2 if Route Error packet
- Public Key: The public key field of the Forwarding Ant will contain the public key of the source while the public key of the backward ant will contain the public key of the destination.
- Digital Certificate: Ensures the source and the destination public keys are untampered. The digital certificate consists of the hash value of the source address and the public key.

The concept of the digital certificate has been changed to see to it that the malicious nodes do not change the public key of the communicating parties. This digital certificate ensures that the source address and the public key are hashed first to generate the message digest. Later on, the hash value is encrypted with the public key of the source and then it is transmitted.

$$\text{Dig} - \text{cert} = \text{EKU}[\text{Hash}(\text{Address},\text{KU})]$$

Hence unless the private key of source is not available, nobody can modify the public key of the source.

A. Confidentiality as the Service

Confidentiality ensures that nobody other than source can read what the data is. Hence the data is supposed to be illegible to all the other intermediate nodes. If the source wants to have confidentiality as the service, communication follows with the destination considering the public key of the destination as the key to be used for Encryption as shown below.

C = EKUB(P)

whereP is the Plain Text, C is the Cipher Text while KUB is the Public Key of B. Hence, since B only has the private key corresponding to the said public key, it can only decrypt the cipher text.

Accordingly P = DKRB(C).

B. Authentication as the Service

Authentication ensures that the data has come from the authentic source only. Hence no impersonation attack has taken place. So hiding the data is not important here. Hence using the private key of the source, if we can encrypt the text, then the same can be decrypted at the other end by the suitable destination. Moreover if in between someone else also reads the data, it is since not confidential, there is no such problem since we have to deal with verification of the source only.

C = EKRA(P) and

P = DKUA(C)

whereP is the plain text, C is the cipher text, KRA is the private key of A, KUA is the public key of A which is already known to B.

C. Both Authentication and Confidentiality

If the requirement of the communication is to achieve both authentication and confidentiality at the same time, then source node can encrypt using the public key of the destination followed by the private key of itself. Hence

C = EPRA(EPUB(P))

The destination has the public key of source (A) and the private key of itself (B) and hence it can decrypt with the following expression:

P = EPUA(EPRB(C)) where PUA refers to public key of A and PRB is
the private key of B.

D. Symmetric Key Cryptography

Above subsections deal with how various security services can be handled with the help of public key Cryptography. In symmetric key cryptography, the requirement is the distribution of the symmetric key. Symmetric key refers to the key which is common for both encryption and decryption. The symmetric key can be distributed with the help of public keys distributed to both the parties using forward and backward ants. Once both parties receive the ants, they may now exchange the symmetric keys. Now it can be seen that the Session Keys can be available from the desired source and destinations only. For several other Authentication related tasks following activities can be carried out.

Send Session key encrypted with the public key of the destination.

Destination will issue a nonce (Random Number) n1, encrypt the nonce with the received Ks and send it to source.

C = EKs(n1)

The destination now transmits the cipher text C.

The source will perform a pre-established function established during the configuration of the network as shown below: C = EKs(f(n1)) This information will be sent to the destination again.

The destination will perform the decryption and verify whether the same nonce n1 is deducible by performing the inverse of the result.

Step 1 is meant for confidentiality. Steps 2, 3 and 4 are meant for Authentication purpose. Then after, the entire process of communication starts.

D. Ending the Session

To end with, the session is supposed to provide the digest of the message. For this Cryptographic Hash or Message Authentication Code related functions can be used. These functions are irreversible. Hence for the entire communication, we can have a single packet which contains the message digest. The message digest is the Integrity check value. Whatever ICV has been generated by the source, the same should be generated by the destination also. If the same value is not generated, then it means that someone has tampered with the data. Since the same ICV cannot be generated for another message, ICV generated by the intruder will not match with the original ICV. Hence there is some attack of the data.

ICV = EKs(Hash(Plaintext))

Here Plaintext refers to the entire text to be sent to the destination.

The destination will perform the hash of the plaintext again to verify whether the hash value is same or not. If it is same, then the data is untampered otherwise the data is tampered with.

4. IMPLEMENTAION RESULTS

The same has been implemented in the Glomosim. Here we have considered the area of 4 sq. km. and have simulated the protocol. We have shown the comparison of the devised Routing Algorithm based on ACO with the other standard routing protocols like DSR, AODV and BELLMAN FORD. The initial results show that for lesser number of nodes, the working of AODV fares better than that of ANT, DSR and BELLMAN FORD as shown in figure 3. As the network becomes dense, it is observed that the ANT based routing works similarto the AODV protocol while the DSR has become relatively efficient. It can be seen from the Figure 4 that as the number of nodes increase within a network, the routing takes almost linear time route the packets from source to the destination.

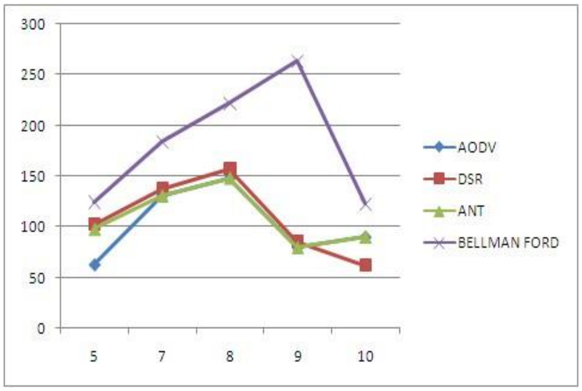

Figure 3. Comparison of Ant based algorithm withDSR, AODV and BELLMAN FORD

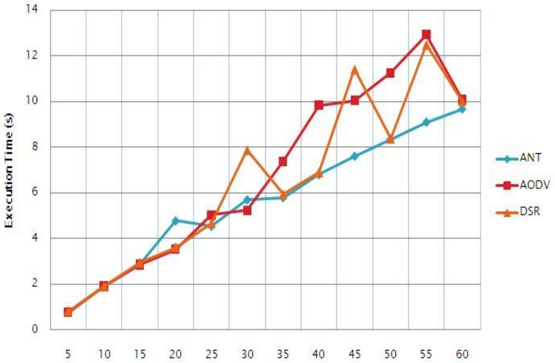

Figure 4. Comparison of the Ant based algorithm with DSR and AODV

Bellman Ford proves to bethe costliest in all cases. The Bellman Ford is costlier due to the implementation of several data structures required to optimize the route between source and the destination and every intermediate node. The Bellman ford employs matrix operations because of which it consumes more time.

5. CONCLUSIONS

The key distribution which has been a major problem with Ad Hoc Networks has been considered and a method to resolve the same has been discussed in this paper. Also care has been taken to incorporate major security services whether it is authentication, confidentiality, both authentication and confidentiality and even symmetric key cryptography. Future scope of this work may involve the cryptographic service called Non-Repudiation. This service deals with the problem of verifying the integrity of the person. If the source denies having sent the message or the destination denies having received the message, it creates a problem with Ad Hoc Networks. Here we do not have any central authority that checks or identifies whether there is any such problem or not as in conventional wired/cellular networks. Future work may deal with this situation.

REFERENCES

[1] SA Arunmozhi and Y Venkataramani, Ddos attack and defense scheme in wireless ad hoc networks, arXiv preprint arXiv:1106.1287 (2011).

[2] Sonali Bhargava and Dharma Agrawal, Security enhancements in aodv protocol for wireless ad hoc networks, IEEE (2001).

[3] Sonali Bhargava and Dharma P Agrawal, Scalable security schemes for ad hoc networks, IEEE (2002).

[4] Ye CHEN, Guo-bo ZHAO, Jun-yong LIU, Tian-qi LIU, and Hua-qiang LI, An ant colony optimization and particle swarm optimization hybrid algorithm for unit commitment based on operate coding [j], Power System Technology 6 (2008), 014.

[5] P Deepalakshmi and S Radhakrishnan, Ant colony based qos routing algorithm for mobile ad hoc networks, International Journal of Recent Trends in Engineering 1 (2009), no. 1, 459–462.

[6] Sanjay Kumar Dhurandher, SudipMisra, Mohammad S Obaidat, and Nidhi Gupta, An ant colony optimization approach for reputation and quality-of-service-based security in wireless sensor networks, Security and Communication Networks 2 (2009), no. 2, 215–224.

[7] Gianni Di Caro, Frederick Ducatelle, Luca Maria Gambardella, and M Dorigo, Anthocnet: an adaptive natureinspired algorithm for routing in mobile ad hoc networks., European Transactions on Telecommunications 16 (2005), no. 5, 443–455.

[8] Marco Dorigo and Mauro Birattari, Ant colony optimization, Encyclopedia of machine learning, Springer, 2010, pp. 36–39.

[9] Marco Dorigo, Mauro Birattari, and ThomasStutzle,¨ Ant colony optimization, Computational Intelligence Magazine, IEEE 1 (2006), no. 4, 28–39.

[10] Tao Jiang and John S. Baras, Ant-based adaptive trust evidence distribution in manet*, Proceedings of the 24th International Conference on Distributed Computing Systems Workshops (ICDCSW04), 2004.

[11] M. Tim Jones, Artificial intelligence application programming, WILEY - Dreamtech Press, 2003.

[12] ShahabKamali and Jaroslav Opatrny, Posant: A position based ant colony routing algorithm for mobile adhoc networks, Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on, IEEE, 2007, pp. 21–21.

[13] Aram Khalili, Jonathan Katz, and William A. Arbaugh, Toward secure key distribution in truly adhoc networks, Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT-w03) (2003), 1–5.

[14] Ramkumar. K.R, Ravichandran. M, Hemachandar. N, ManojPrasadh. D, and GaneshKumar. M, Raam: Routing algorithm using ant agents for manets, ICACT, 2009.

[15] Haiyan Luo and Petr, Self securing ad hoc wireless networks, Seventh International Symposium on Computers and Communications (ISCC02), 2002.

[16] Kenji Miyao, Hidehisa Nakayama, Nirwan Ansari, Yoshiaki Nemoto, and Nei Kato, A reliable topology for efficient key distribution in ad-hoc networks (an invited paper), IEEE (2008).

[17] B Chandra Mohan and R Baskaran, A survey: Ant colony optimization based recent research and implementation on several engineering domain, Expert Systems with Applications 39 (2012), no. 4, 4618– 4627.

[18] C. Siva Rama Murthy and B. S. Manoj, Ad hoc networks protocols and architecture, Pearson Education, 2005.

[19] EseosaOsagie, ParimalaThulasiraman, and Ruppia K Thulasiram, Paconet: improved ant colony optimization routing algorithm for mobile ad hoc networks, Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on, IEEE, 2008, pp. 204–211.

[20] Roberto Ki Pietro, Luigi V Mancini, and SushilJajodia, Efficient and secure key management for wireless mobile communications, POMC, 2002.

[21] Chandrasekar Ramachandran, SudipMisra, and Mohammad S Obaidat, Fork: A novel two-pronged strategy for an agent-based intrusion detection scheme in adhoc networks, Computer Communications 31 (2008), no. 16, 3855–3869.

[22] William Stallings, Cryptography and network security principles and practice, Pearson Education, 2000.

[23] Michael Steiner, Gene Tsudik, and Michael Waidner, Cliques: A new approach to group key management, In proceedings of the 18th International Conference on Distributed Computing Systems (ICDCS98), 1998.

[24] Jianping Wang, EseosaOsagie, ParimalaThulasiraman, and Ruppa K Thulasiram, Hopnet: A hybrid ant colony optimization routing algorithm for mobile ad hoc network, Ad Hoc Networks 7 (2009), no. 4, 690–705.

[25] Panlong Yang and Shaoren Zheng, Security management in hierarchical ad hoc networks, IEEE (2001).

[26] SaadGhalebYaseen and Nada MA Al-Slamy, Ant colony optimization, IJCSNS 8 (2008), no. 6, 351.

DOI: 10.090592/IJCSC.2015.613