A Trust Conscious Secure Route Data Communication in $MANET_S$

Dr. Anil Kapil anil_kdk@yahoo.com
Professor, M M Institute of Computer Technology and Business Management, M M University, Mullana, Ambala, Haryana, India

Mr. Rajneesh Gujral rgujral77@yahoo.com
Asst. Professor, Department of Computer Engineering, M M Engineering College, M M. University, Mullana, Ambala, Haryana, India

ABSTRACT

Security in mobile adhoc networks is difficult to achieve, notably because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, the absence of a certification authority, and the lack of a centralized monitoring or management point. The major difficulty in adhoc network occurs when a new node join network but not having any trust based relation with other nodes of network. We have proposed a new mechanism that provides trust conscious secure route data communication between the Mobile nodes. In this mechanism we will dynamically increase the trust from (Low to High) between the mobile nodes using proxy node. When mobile node needs secure data communication, it will generate a dynamic secret session key with the desired destination mobile node directly or via proxy mobile nodes. These dynamic secret session keys are generated using message digest and Diffie-Hellman protocol.

Keywords: Session keys, Message digest, MANETs.

1. INTRODUCTION

$MANET_S$ are made up of collaborative mobile nodes equipped with wireless network interfaces, where each node is able to communicate with other nodes within its transmission range without any fixed infrastructure, such as a name server or switches to set up connections The security services of adhoc networks are not together different from those of other network. The goal of these services is to protect information and resources from attacks and misbehavior. These security services such as privacy, integrity and authentication cannot be achieved without a prior solid key management. The major problem in providing security service in adhoc networks is how to manage the key that provide trustworthiness and privacy in data communication. In order to design practical and efficient key management system, it is necessary to understand the characteristics of adhoc networks and why traditional key management system is not suitable to such environments. To establish a secure communication between two mobile nodes in an adhoc manner, i.e. secure peer- to -peer communication, it is necessary for the two nodes to share a secret key [1]. This can be easily achieved if we assume the existence of a public key infrastructure (PKI) [2, 3]. However, many mobile adhoc networks cannot afford to deploy public key cryptosystem due to their high computational overheads. In mobile adhoc networks, due to

unreliable wireless media, mobile node mobility and lack of infrastructure, providing secure communications is a big challenge. The symmetric key cryptography approach has computation efficiency because the algorithms are less complex and key size is small. In fact, any cryptographic means is ineffective if the key management is weak. We have proposed to implement our mechanism on reactive routing protocols, since they are more appropriate for wireless environments and they initiate a route discovery process only when data packets need to be routed [4]. Discovered source route are then cached until they go unused for a period of time, or break because of the network topology changes [5]. This paper is organized as follows the next two sections presents some of related works and overview on AODV protocol with different trust based scenarios. Section 4 gives the proposed mechanism on reactive protocol AODV.

2. RELATED WORKS

A reputation based trust management scheme for peer to peer systems has been presented in [6] [7].Here a node's trust is calculated from the reputation based on complaints lodged by its previous clients. A similar scheme with local and global reputation is discussed in [8].The distributed trust model in a general network scenario based on human approach of knowing about strangers from friends, is decentralized [9].A modified hierarchical trust Public key model, of which nodes can dynamically assume management roles, to present a framework for key that provides redundancy and robustness between pairs of nodes [10] .Similar certificate path discovery in hierarchical PKI trust model in MANET. This approach labels each CA certificate with codeword. By using the label, it designs an algorithm to speed up the process of certificate path discovery without the presence of central PKI service [11]. Another model presented for calculating Direct & Situational Trust values can be shared among neighbours using a higher layer Repudiation Exchange Protocol in [12][13]. In Gehramannet al. [14] describe a set of techniques to help two wireless devices to securely authenticates each others and agree on a shared data string via insecure wireless channel. In similar work [1], Sencun zhu et al. present a scalable and distributed protocol that enables two nodes to establish a pair-wise shared key on the fly, without requiring the use of any online key distribution center. The design of their protocol is based on a novel combination of two techniques: probabilistic key sharing and threshold secret sharing. Wen Liang Du and jing Deng [16], have also presented a new pair-wise key pre-distribution scheme for wireless sensor networks. Their scheme has a number of appealing properties. It is scalable and flexible, and nodes do not need to be deployed at the same time, that's to say they can be added after initial deployment, and still be able to establish secret keys with existing nodes. The same approach is presented in [1] for establishing a pair-wise shared key between two nodes. Each node is pre-loaded with unique key that it shares with the KDC. To communicate securely, a pair of participants obtains fresh session keys from the online server. For example, secret key protocols such as Kerberos [17] and otway-rees [18] require an interactive trusted third party, a KDC, or a key Translation center (KTC) in order to establish a shared by between any two nodes. While these schemes have been widely deployed in wired networks, this approach is not suitable for adhoc networks that are characterized by dynamic topology changes and node failures, disconnections from the network and by the fact that there is typically no online server available.

3. AODV WITH EMBEDDED SECURITY

An AODV is a reactive adhoc on demand distance vector routing protocol. In this protocol, when a node joins the network and communicates with another node, it broadcasts a route request or REQUEST packet to its neighbors. The REQUEST is propagated from neighbors to neighbors and so on, using controlled flooding. The REQUEST packet set up a reverse path to the source based on intermediate routers that forward this packet. If any intermediate node has a path already to the REQUEST destination, then this intermediate node replies with a Route Reply or REPLY packet, using the reverse path to the source. In this paper, we embedded the security requirement on AODV routing protocol using trust level. A trust level of network is defined on the bases of session keys between the nodes. Three different possible scenarios can occur. F**irst scenario,** when adhoc network is recently establishes (**Trust level equal to Low)** and a mobile

node communicates with specific destination. Source node broadcast route REQUEST and then find the shortest route with destination node either directly or through intermediate nodes using AODV protocol. Then pair-wise session keys are established between all the intermediate nodes (if any) using diffe-hellman protocol. Finally, session key will be established between source and destination nodes for secure communication. **Second scenario (trust level between Low to High):** This scenario happens when the Adhoc network is already existing but the trust is not equal to High (varies between Low to high). When a source node sends a REQUEST packet to a specific destination, the intermediate node checks that is their any long trust pairing with the generator node of the actual request using AODV protocol. In this case, the route discovered by AODV between two nodes may not be the shortest route in terms of hop-count, as shown in figure1. However, AODV was able at least to find a route with a guarantee of security and key pairing between the nodes. If all the nodes on the shortest path (in term of hop count) between two nodes can satisfy the pair- wising requirements, AODV will find route that are optimal. AODV security restrictions may force packets to follow longer, but more secure paths. **Third scenario (Trust level equal to High)** First, let's consider the case when all nodes have a shared key with all their neighbor's node in the adhoc network i.e. the trust level is equal to high. In this case, our protocol will behave exactly like any traditional on-demand adhoc routing protocol in finding the destination node when the source node starts the REQUEST. In this case, the route found will be optimal in terms of security requirements and hop count. A fundamental issue that must be addressed in this case, is that every node is sharing (N-1) keys with others nodes, where N is the number of nodes in the network. Clearly, this scheme is not suitable for large networks since the storage required per node increase linearly with the network size.

4. THE PROPOSED MECHANISM

In this paper, we used an adhoc On-Demand routing protocol (AODV) to find the secure route through trusted intermediate nodes which have a secret shared key. Hence, our modification to the traditional adhoc routing protocol changes routing algorithm. The route discovered by our mechanism between two nodes may not be the shortest route in term of hop-count, as we show in figure1. At least, in our mechanism AODV is able to find a route with guarantee of security if one or more routes that satisfy the required security attributes exist then it will find the shortest secure route. If insecure route exist between two nodes (source & destination node), then our mechanism initiates a session key which generate a secure route directly or with intermediate nodes.

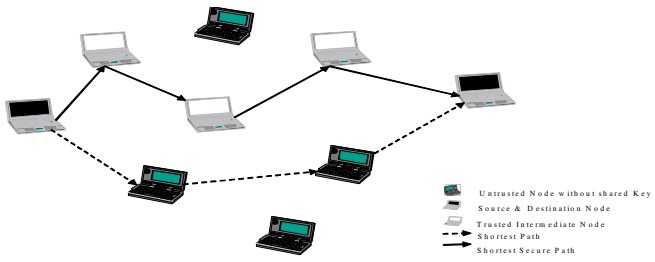


FIGURE 1: Shared key secure route in adhoc network

For establishing a long term secret between two mobile nodes first exchange their initial authentication information then establish the session key between the mobile node with Diffe-Hellman algorithm at run time. Our approach we will show two scenarios.

- Joining a new node in adhoc network and Trust relationship nil.
- A trusted Intermediate mobile node acting as a Proxy Node.

Let's imagine that the new mobile node A join the Adhoc network and wants to communicate with node that is within its range. Suppose the mobile node B is in range of mobile node A. Then the

following Packets will flow between mobile node A and mobile nodes B for secure route data communication. The proposed mechanism used some notation shown in TABLE 1.

4.1 Joining a new node in adhoc network and Trust relationship nil.

Step1: Initially mobile node A generates ticket for authentication to mobile node B .The mobile node A sends a ticket to mobile node B that contain

$A \rightarrow B : ID_{A,} h(K_A)$

.i.e. ID_A and hash of the number K_A .The K_A is generated by Diffie-Hellman Protocol at run time.

$K_A = (G^X \bmod N)$

Step2. Same way mobile node B sends ticket to mobile node A for authentication. The ticket contains

$B \rightarrow A : (ID_B, h(K_B))$

where, $K_B = (G^Y \bmod N)$

Step3. When mobile node A want secure communicate with mobile node B. Mobile node A generate ticket for mobile node B that contain

$A \rightarrow B : (ID_A, K_A, N_A)$

Then mobile node B use hashing algorithm and make the hash of K_A key i.e. $(h(K_A))$ compare both the hash if they are equal send reply ticket to mobile node A.

TABLE 1: Notation

G	Large size prime public number (public to every Adhoc networks node)
N	Large size public prime number i.e. $\frac{N-1}{2}$ is also a prime number
A , B, C	Mobile node A, mobile node B and mobile node C
ID_A	Identity of mobile node A
h (K_A)	The Hash Function of the Shared key K_A
K_{AB}	The Shared key between mobile node A and B
E_{AB}	Encryption using the shared key between mobile node A and B
N_A , N_B , N_C	Large random numbers selected by mobile nodes A, B and C respectively
$A \rightarrow B$	Message from mobile node A to mobile node B
(G, N)	Universally used Large prime numbers in adhoc network
(X, Y)	Secret large random numbers used by Mobile Nodes

Step4. Mobile node B sends reply ticket that contains plain text form ID_B , K_B and encrypted ticket $E_{AB} (ID_B , N_A , N_B , h(K_B))$.

$B \rightarrow A : \{ID_B, K_B, E_{AB}(ID_B, N_A - 1, N_B, h(K_B))\}$

Mobile node A receive K_B and calculate hash of K_B i.e. $h(K_B)$ and compare it with previous hash if match occurs it prove the authentication of mobile node B. Then mobile node A decrypt the ticket by secret shared key E_{AB} and check the random number N_{A-1}. It proves that the ticket is sent by mobile node B.

$E_{AB} = G^{XY} \bmod N = K_A^Y \bmod N = K_B^X \bmod N$

Step5. Mobile Node A send acknowledgment ticket to mobile node B that contain.
$A \rightarrow B : E_{AB}(ID_A, N_{B-1})$

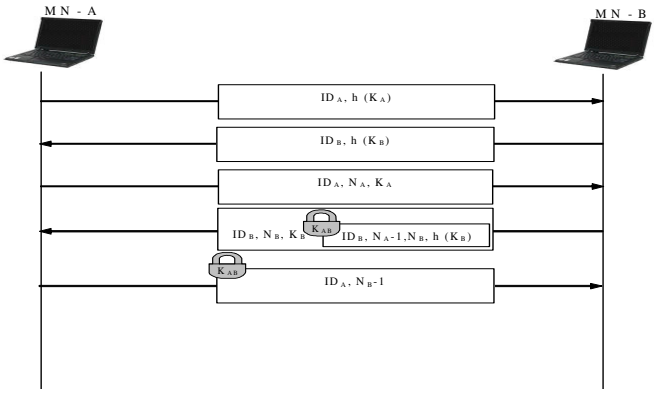
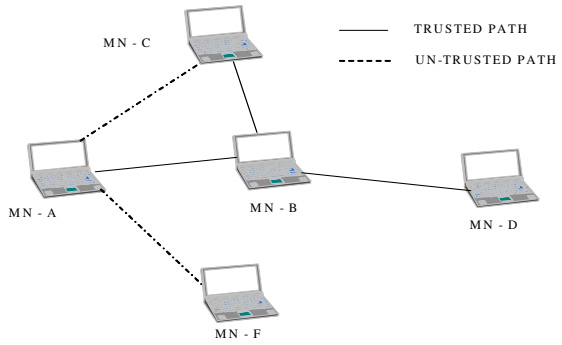


FIGURE 2: Secure Route Data Communication between Mobile Node A and Mobile Node B

4.2 A trusted Intermediate Node act as a Proxy Node

The adhoc routing protocol AODV that embedded security has presented in the section 4.1 was described only for two nodes in the same transmission range, and the procedure to establish a shared secret between them without any intermediate node. Imagine that there is nearby another mobile node C that wants to use this service. The two nodes will assist this node to establish the pair-wise keys. Let's suppose that mobile node C can communicate only with mobile node B in secure manner, and mobile node B has also a pair-wise with mobile node A. Since mobile node C shared a long term trust with mobile node B and they have a Pair-wise Key K_{BC}, mobile node B will take over to facilitate the establishment of pair-wise between mobile node C and A to Communicate with their common shared long term secret K_{AC}.We will notice through the details which will be presented in the next subsection, that mobile node B in the middle act as a proxy between mobile node A and C by forwarding the identity and the Diffie-Hellman hash of the new mobile node C to the node.



FIGHURE 3: Mobile Node B acting as Proxy Node

In this section we presented the mechanism extend the trust level of the mobile node in adhoc network in secure manner. Let's consider again the adhoc network described in figure 3. Suppose the mobile node C in the network, which for the instance contains only a trust relation with mobile node B, wishes to establish a trust relation with mobile node A .If we suppose that the mobile adhoc network contains only these three nodes, then we will increase the trust level of the network from 0 to 66 percent up to 100. We will describe in detail how to establish a trust relation in the following massages exchanged between the three nodes.

Step1: Mobile Node C broadcasts a REQUEST packet to mobile node A with its identity and its hashed Diffie-Hellman secret. When mobile node B receives this request and trusts the originator mobile node C, it forwards the identity of mobile node C and its hashed Diffie-Hellman secret to mobile node A which it trusts also.

Step2: Mobile Node A, which trusts mobile node B, will send a REPLY packet with its hashed Diffie–Hellman secret to mobile node B. This last will forward this reply from mobile node A to mobile node C. We notice that mobile node B is just acting as a proxy between mobile nodes C and mobile node A in order to establish a temporary communication channel between the two nodes.

Step3: Mobile Node C sends REQUEST Ticket with its identity $\mathrm{ID_C}$ and $\mathrm{K_C}$ to mobile node A via mobile node B.

$$\mathrm{C \rightarrow A : ID_C, K_C}$$

Step4: Mobile Node A verifies $\mathrm{K_C}$ based on $h(K_C)$. Then, it computes the shared key $\mathrm{K_{AC}}$ as a hash $\mathrm{h(G^{CA} \bmod N)}$. Mobile Node A picks a random $\mathrm{N_A}$; encrypts and authenticates $\mathrm{N_A}$, $\mathrm{h(K_A)}$ and its identity $\mathrm{ID_A}$ using $\mathrm{K_{AC}}$, and inserts the result into the REPLY packet, and finally sends the result along with $\mathrm{ID_A}$ and $\mathrm{K_A}$ to mobile node C via mobile node B.

$$\mathrm{A \rightarrow C : ID_A, K_A, E_{CA}\{ID_A, N_A, h(K_A)\}}$$

Step5: Node C receives $\mathrm{K_A}$ and computes the shared key $\mathrm{K_{AC}}$ as a hash $\mathrm{h(G^{CA} \bmod N)}$. Then, extracts $\mathrm{N_A}$ & $\mathrm{h(K_A)}$, and verifies $\mathrm{K_A}$ based on $\mathrm{h(K_A)}$, picks a random $\mathrm{N_C}$ and encrypts and authenticates $\mathrm{ID_C}$, $\mathrm{N_C}$ and $\mathrm{N_A}$ using $\mathrm{K_{AC}}$ and sends the result to node A in another REQUEST packet.

$$\mathrm{C \rightarrow A : E_{CA}(ID_A, N_C, N_A)}$$

Step6: Node A decrypt using $\mathrm{K_{AC}}$ extracts $\mathrm{N_C}$ and sends it to node C.

$$\mathrm{A \rightarrow C : N_C}$$

At this sage both C and A can calculate a shared secret key that can use to communicate securely.

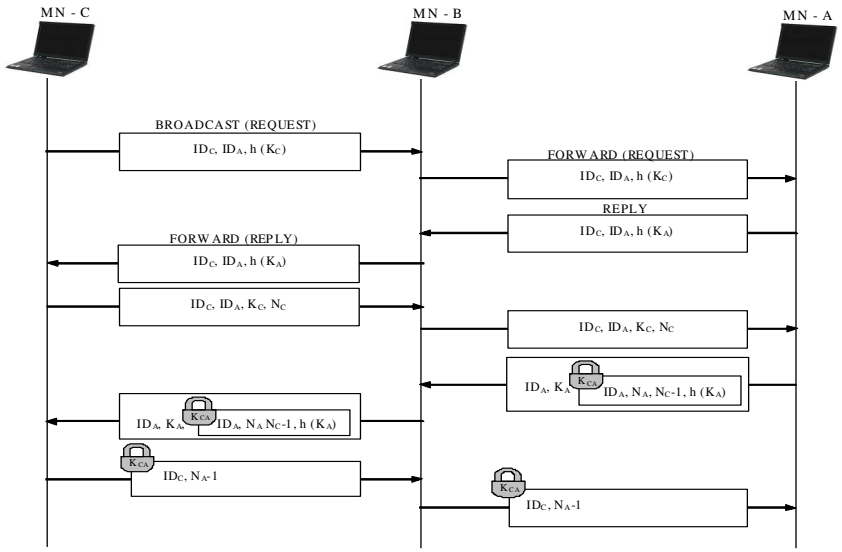


FIGURE 4: Secure Route Data communication between Mobile node C and mobile node A via Proxy mobile node B.

5. CONCLUSION & FUTURE WORKS

In most key management protocols, a trusted party is needed to act as a trust proxy node. Due to the dynamicity of adhoc networks, such central entity may easily become compromised or leave

the network. Thus, we focused in our work on proposing approach on demand protocol which enables two nodes to autonomously establish a shared key to secure further communication. Our approach is easily scalable to dynamically increasing trust directly or through proxy nodes. In future work we will add the mechanism that computes the direct Trust in a node. The accuracy & sincerity of the immediate neighboring nodes is measured by observing their contribution to the packet forwarding so that no node perform selfishness during data transfer from sender to receiver node.

6. REFERENCES

1. Sencun Zhu, Shouhuai Xu, Sanjeev Setia, Sushil jajodia , *"Establishing Pairwise Keys for Secure Communication in Adhoc Networks :A Probabilistic Ap*proach",p.p 326-331,ICNP 2003.
2. R. Housley, W. Ford, W. Polk and D. Solo, "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*." http:/www.faqs.org/rfcs/rfc2459.hunl, January 1999.
3. S. Yi and R. Kravets, "*Key Management for Heterogeneous Adhoc Wireless Networks*", IEEE ICNP'02, pp 12-15, Nov.2002.
4. C. E. Perkins and E. M. Royer," *Adhoc Networking, Adhoc On-Demand Distance Vector Routing*.",Addison-Wesley, 2000.
5. D. B. Johnson, D. A. Maltz, and 1. Broch," DSR :*The Dynamic Source Routing Protocol for Multi-Hop Wireless Adhoc Networks.",* In Adhoc Networking, ch. 5, p.p. 139-172. Addison-Wesley, 2001
6. K. Aberer and Z. Despotovic," *Managing Trust in a Peer-2-Peer Information System*.", In Proceeding of the Xth International Conference on Information and Knowledge Management, 2002.
7. K. Aberer: P-Grid, "A *self organizing access structure for P2P information system*.", In Proceeding of COOPIS, 2001.
8. B. Yu and M.P. Singh," *An Evidential Model of Distributed Reputation Management*.", In Proceeding of AAMAS 02, Bologna, Italy. Publication: ACM Press July 15-19 2002.
9. A. Abdul-Rahman and S.Hailes:" *A Distributed Trust Model In New Security Paradigma"* Workshop 1997, ACM 1997.
10. Hadjichristofi, G.C., Adams, W.J., Davis, N.J., IV, *" A framework for key management in mobile adhoc networks*", In Proceeding of the International Conference on Information Technology: Coding and Computing , IEEE Computer Society, Volume 2, pp.568-573, April 2005.
11. He Huang, Shyhtsun, Felix Wu, " *An approach to certificate path discovery in mobile adhoc networks"* , In Proceeding of the 1st ACM Workshop on Security of Adhoc and Security of adhoc and Sensor Networks, ACM, p.p.1-53,2003.
12. A.A. Pirzada,A.Datta,and C. McDonald, *" Propagating Trust in Pure Ad-hoc Networks for reliable Routing*" , In Proceeding of the International Workshop on Wireless Ad-hoc Networks (IWWAN),2004.
13 A.A. Pirzada, A.Datta, and C. McDonald, *"Trust Based Routing for Ad-hoc Wireless Networks*", In Proceeding of the IEEE International Conference on Networks (ICON'04), p.p. 326-330,2004.
14 Christian Gehrmann and Chris 1. Mitchell, "*Manual authentication for wireless devices*", Cryptobytes 2004, volume 7 No.1, 2004.
15. ENLIANG Du, JING Deng, "*A Pairwise Key Pre·Distribution Scheme for Wireless Sensor* Networks", In Proceeding of the 10th ACM conference on Computer and communications security p.p. 42-51, 2003.
16. Koh I and B. Neuman, "*The Kerberos Network Authentication Service"* (V5). RFC 1510, September 1993.
17 D. Otway, O. Rees, "*Efficient and Timely Mutual Authentication*, Operating Systems" Review, 21 (1987).