Journal of Computer Science 3 (12): 939-943, 2007
ISSN 1549-3636

# Secure Antnet Routing Algorithm for Scalable Adhoc Networks Using Elliptic Curve Cryptography

V. Vijayalakshmi and T.G. Palanivelu
Pondicherry Engineering College, Pondicherry-605 014, India

**Abstract:** The secure end-to-end route discovery in the decentralized Mobile Adhoc Networks (MANETs) should have to meet the requirements of prevention of DoS attacks on data traffic, should be adaptive and fault tolerant and must have high speed, low energy overhead and scalability for future development. In this research a secure routing using antnet mechanism and mutual authentication using Elliptic Curve Cryptography (ECC) has been proposed to meet the above requirements. The common perception of public key cryptography is that it is not well suited for adhoc networks as they are very complex and slow. Against this popular belief, this research implements Elliptic Curve Cryptography - a public key cryptography scheme. ECC provides a similar level of security to conventional integer-based public-key algorithms, but with much shorter keys. Because of the shorter keys ECC algorithms run faster, require less space and consume less energy. These advantages make ECC a better choice of public key cryptography, especially for a resource constrained systems like MANETs. Using the antnet routing algorithm, the highly trustable route will be selected for data transfer and each Mobile Node (MN) in MANET maintains the trust value of its one-hop neighbors. The mutual authentication between source and destination is done by master key exchange using Elliptic Curve Cryptography (ECC).

**Key words**: Mobile Adhoc Networks (MANETs), Elliptic Curve Cryptography (ECC), cluster head, virtual cluster, centralized authority, mobile node, Message Authentication Code (MAC)

## INTRODUCTION

Adhoc networks have enormous impact on many aspects such as emergency medical care and military services where security of data is very important. The secure path establishment procedure plays a vital role in the MANET security mechanism. The efficiency of secure route discovery will be evaluated by the factors like prevention of DoS attacks on data traffic, high speed, low energy overhead and successful secure link establishment among neighbors. The flat network layout is good for small networks but does not scale well with increase in network size since the nodes in the neighborhood of the base station are flooded by route requests and replies. Also in large networks the average number of hops to the base station increases, which means the energy consumption for route requests and replies, increases drastically. Due to larger distances, the end-to-end data latency also increases. In order to overcome these problems, ECC security mechanism[1-3] and a prediction based proactive hierarchical network[4] structure has been considered.

This research focuses on establishing efficient secure routing in clustered based adhoc networks by a two fold process viz.,

- Estimation of trust values of neighbors[5]
- Secure end-to-end route discovery using Antnet routing mechanism[6] and mutual authentication using ECC[7].

In this secure routing mechanism, each MN in the cluster maintains the trust value of its one-hop neighbors. Trust is nothing but the measure of uncertainty about the node (trust value is associated to successful packet forwarding) and it can be measured by entropy. In this research the trust relationship of neighborhood node is evaluated by the recommendation of third party. That is, by observing the trust value of the third party for the particular packet transmission, the trust value of neighbors can be predicted. The secure path will be evaluated and established using ECC since it offers an excellent level of security with lower key sizes.

## SCALABLE CLUSTERING NETWORKS

The efficiency of the routing algorithm depends upon the structure of network. The scalability will be achieved by considering the proactive way of prediction

**Corresponding Author:** V. Vijayalakshmi, Pondicherry Engineering College, Ponicherry-605 014, India

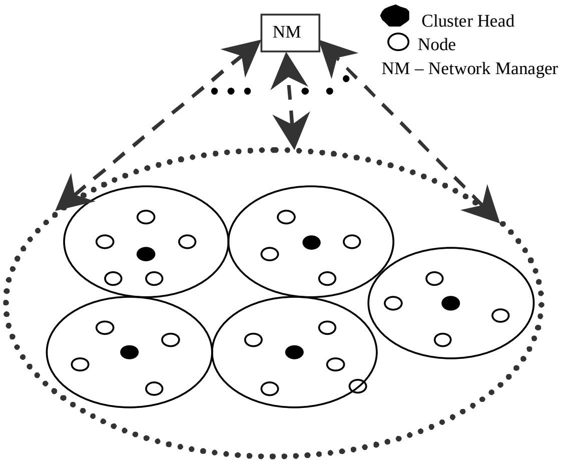

Fig. 1: Hierarchical structure of clustering model

method during cluster formation. Using this method, security architecture can be updated from small scale to large-scale networks. That is, the entire network will be divided into many clusters. Cluster Head (CH) manages each cluster. All CHs are connected to Network Manager (NM). CHs are also an ordinary communication node with additional tasks such as collecting and processing the data from their cluster members and forwarding the results towards the NM. It will be changeable according to mobility. The considered scalable hierarchical structure shown in Fig. 1 has clusters of sensor nodes based on prediction based proactive model.

The idea behind this model are Virtual Cluster Concept, ($P_{xk}$, $T_{xk}$, $D_{xk}$) -Clustering approach and Mobility prediction model[4].

## SECURE ROUTE DISCOVERY

**Trust estimation:** This section deals with the trust estimation of the neighborhood nodes. The basic understanding of the trust is summarized as follows:

- Trust is a relationship established between two entities for a specific action. In particular, one entity trusts the other entity to perform an action. In this study, the first entity is called the subject, the second entity is called the agent. So, the notation used to describe a trust relationship is {subject: agent; action}

Let T {subject: agent; action} denote the trust value of the trust relationship {subject: agent; action} and P{subject: agent; action} denote the probability that the agent will perform the action in the subject's point of view. Information theory states that entropy is a measure of uncertainty; thus, the entropy-based trust value as

**Error!**

$$T\{\text{trust}: \text{agent}, \text{action}\} = \begin{cases} I - H(p), \text{for } 0.5 \le p \le 1 \\ H(p) - 1, \text{for } 0 \le p < 0.5 \end{cases} \qquad (1)$$

where,

$H(p) = -\, p \log_2 p - (1-p) \log_2 (1-p)$
$P \quad = P$ {subject: agent; action}

In this work, the trust value is a continuous real number [-1, 1]. This definition satisfies the following properties.

- When P = 1, the subject trusts the agent the most and the trust value is 1
- When P = 0, the subject distrusts the agent the most and the trust value is -1
- When P = 0.5, the subject has no idea about the agent and the trust value is 0

In general, trust value is negative for $0 \le P < 0.5$ and positive for $0.5 \le P \le 1$. Trust value is an increasing function with P. It is a one-to-one mapping between T {subject: agent; action} and P {subject: agent; action}.

One typical example, A wants to establish the trust relationship with B (A and B are two nodes) based on A's previous observation about B. In this action, A asked B to forward N-number of packets and B in fact forwarded K-number of packets.

Let V ( i ) be the performance action of the B at the i<sup>th</sup> trial. That is, if V( i ) = 1, B correctly performs the action at the i<sup>th</sup> trial; Otherwise V( i ) = 0. n (N) = $\sum_{i=1}^{N} V_i$ → Number of actions successfully performed by B out of totally N trials. For the N trials of transmission between two nodes, K trials are success. The probability of successfulness of $(N+1)^{th}$ trial will be predicted by Bayesian Theorem given below

$$P(v(N+1)=1/n(N)=k = \frac{P(v(N+1)=1, n(N)=k)}{P(n(N)=k)} \qquad (2)$$

Here the probability of all trials will be calculated by the Bernoulli's distribution given below

$$P\{n(N)=K\} = \left( {}^{N}_{K} p^{K} (1-p)^{(N-K)} \right. \qquad (3)$$

where,

P = Average Probability of success transmission of each packets
N = Total number of packets transmitted by source
K = Number of packets successfully transmitted by neighborhood nodes

**Secure route establishment using antnet:** When a node (source) wants to establish a route to the other node (destination), the source first tries to find multiple routes to the destination. Then the source tries to find the packet-forwarding trustworthiness of the nodes on the routes from its own trust record or through requesting recommendations. Finally the source selects the trustworthy route to transmit data. After the transmission, the source node updates the trust records based on its observation of route quality. Using Antnet algorithm the following sequence of steps leads to discovery of route:

- Each source launches some forward agent packets to destination through multi hop propagation. The path will be selected randomly based on the current routing table
- The forward agent packets create a stack, pushing in trip times, trust values and traffic intensities of every node it visits during transmission as shown in Fig. 2a
- When the packets reach the destination, some backward agent packets will be sent to the source. During this time, the backward agent packets inherit the stacks parameters. That is pop the parameter and verify once again as shown in Fig. 2b
- The backward agent packets deliver the parameters of trust values, traffic intensities and delays of discovered routes to source. Finally the source will select the optimum path to destination[8-9]

The secret-key exchange between the source and destination followed by ECC is shown in Fig. 3.

G → Point on Elliptic Curve whose order is ‘n’
N → Total number of points in Elliptic Curve including point on infinity[7]
$N_A, N_B$ → Secret Keys
$P_A, P_B$ → Public Keys

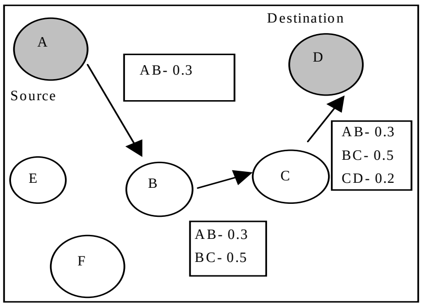

Fig. 2 (a): Forward route discovery

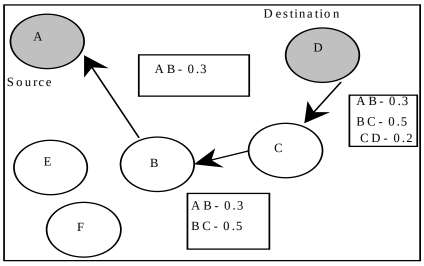

Fig. 2 (b): Backward route discovery

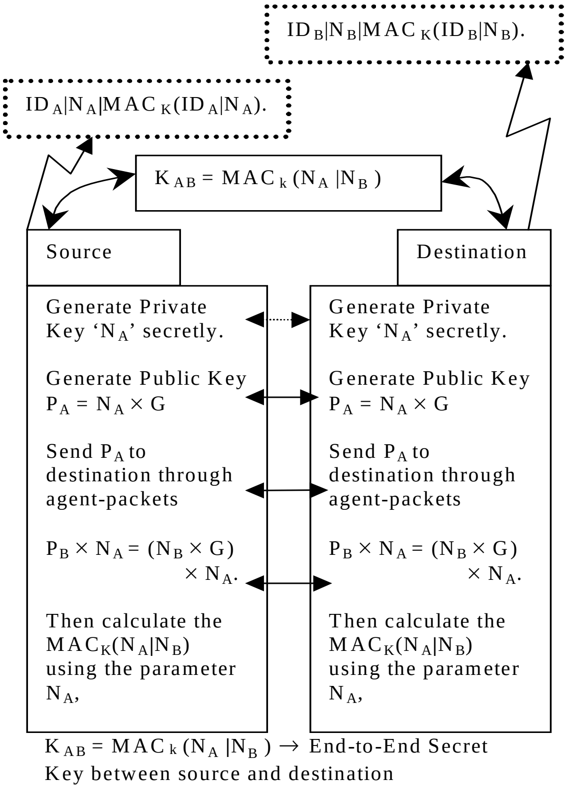
ID_B|N_B|MAC_K(ID_B|N_B).
ID_A|N_A|MAC_K(ID_A|N_A).
K_AB = MAC_k (N_A |N_B )
Source
Destination
Generate Private Key ‘N_A’ secretly.
Generate Private Key ‘N_A’ secretly.
Generate Public Key P_A = N_A × G
Generate Public Key P_A = N_A × G
Send P_A to destination through agent-packets
Send P_A to destination through agent-packets
P_B × N_A = (N_B × G) × N_A.
P_B × N_A = (N_B × G) × N_A.
Then calculate the MAC_K(N_A|N_B) using the parameter N_A,
Then calculate the MAC_K(N_A|N_B) using the parameter N_A,
K_AB = MAC_k (N_A |N_B ) → End-to-End Secret Key between source and destination

Fig. 3: Session secret key negotiation algorithm

## RESULTS AND DISCUSSION

The prediction based proactive cluster formation and the novel idea of secure route discovery method has been implemented and simulated in Network Simulator (NS-2) by assuming the parameters shown in Table 1.

Table 1: Assumed parameters for simulation

| Total No. of nodes including CH | 40 |
|---|---|
| Number of clusters | 4 |
| Nodes per cluster | 10 |
| Total network area | 1 Square Km |
| Speed of the node | 0 - 50 $ms^{-1}$ |
| Packet size | 250 to 500 bytes |
| Data rate and type | 100 Kbps and VBR |
| Elliptic Curve | Elliptic curve over binary field, GF($2^m$), 312 bit key size |
| Power required to transmits one packet | 5 mw |

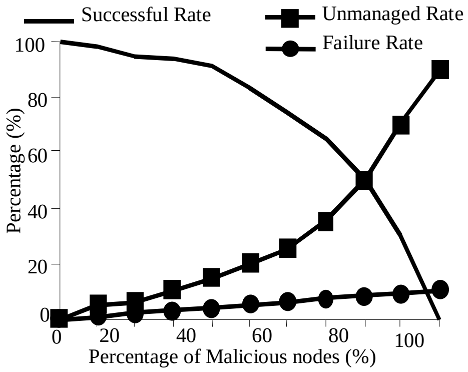

Fig. 4: Stability analysis of proposed routing algorithm

**Packet forwarding performance:** Figure 4 shows the performance of proposed antnet routing algorithm using ECC in the prediction based clustering networks.

The performances have been analyzed with the parameter of percentage of malicious nodes in the cluster network. That is number of dishonest nodes in the cluster. Here the unmanaged rate denotes that number of packets which cannot reach the destination within the desired time and these packets are stored in the honest nodes not dropped. The failure rate denotes percentage of packets dropped by the dishonest nodes and these packets are not available for any other nodes (considered loss of packets).

**Authentication cost ratio:** Authentication is the additional process in the route discovery. Figure 5 and 6 shows the performances of authentication cost ratio, which are obtained by the following computation:

$$\text{Authentication cos t ratio} = \frac{t_{PRO}}{t_{ECC}} \times 100$$

where,

$t_{PRO}$ → processing at every node during route discovery without authentication

$t_{ECC}$ → processing at every node during route discovery with ECC authentication

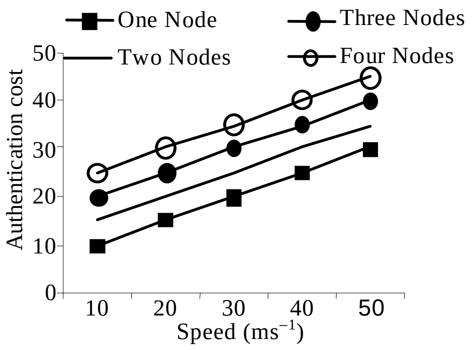

Fig. 5: Authentication cost ratio (intra-domain)

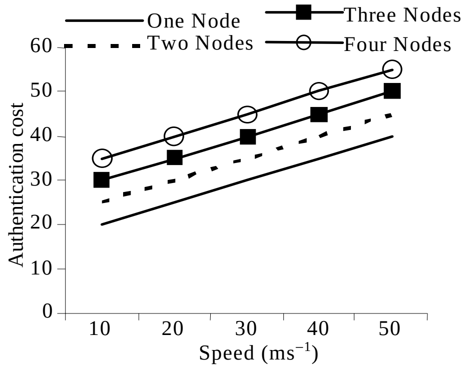

Fig. 6: Authentication cost ratio (inter-domain)

**Trust estimation:** Table 2 discusses the situation that the trust value of neighbors is between 0.1 and 0.4. Normally the range of trust values are between -1 and +1. If the trusts value is negative, the node considers the neighborhood node as a malicious node and if it is positive, the neighborhood node is considered to be a honest node and if it is 0, the node does not have any idea about the neighborhood node. In the cases of positive trust values, the trust value above 0.5 of a particular node has no more questions to the trust algorithm and it considers the node as fully trusted.

If the trust value is between 0.1 and 0.4, the algorithm has perplexity to believe the node. In these cases the trust value of third party has to be considered to believe the neighborhood node. That is trust value of neighborhood node of the neighborhood node is considered. Table 2 shows the trustworthiness of neighborhoods with the help of third party.

Table 2: Trust estimation using third party

| Trust value of third party | Neigh bor‘s trust value T= 0.1 | Neigh bor‘s trust value T= 0.2 | Neigh bor‘s trust value T= 0.3 | Neigh bor‘s trust value T= 0.4 |
|---|---|---|---|---|
| T=0.3 | N T | N T | N T | N T |
| T=0.4 | N T | N T | N T | N T |
| T=0.5 | N T | N T | N T | N T |
| T=0.6 | N T | N T | T | T |
| T=0.7 | N T | T | T | T |
| T=0.8 | T | T | T | T |
| T=0.9 | T | T | T | T |
| T=1 | T | T | T | T |

NT ----- Not Trusted
T ----- Trusted

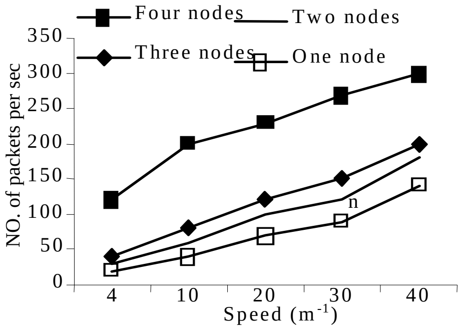

Fig. 7: Necessary packet rate vs speed

**Necessary packet rate vs speed:** Figure 7 shows the performances of the necessary end-to-end packet rate under the mobility consideration. Here four nodes are considered for a particular central node and each curve shows that among the four neighborhood nodes, one node is in mobile with various speed and two nodes are in mobile with various speed and etc. The speed of the node has been considered from 0 to 40 meters per second

## CONCLUSION

The efficient end-to-end route discovery using antnet routing algorithm with master secret key exchange using ECC has been proposed and imposed on the cluster based scalable adhoc networks. Results show that the algorithm will tolerate up to 80% of malicious nodes in the cluster with successful rate of 60%. Even though the percentage of malicious node increases above 80%, the failure rate is very lesser in percentage (below 10%). This novel idea of secure routing algorithm is compatible for instant access networks in Military applications. The results obtained using Network Simulator indicate that the proposed method is practically feasible.

## REFERENCES

1. Lauter, K., 2004. Microsoft corporation, The Advantages of Elliptic Curve Cryptography for wireless security, IEEE Wireless communication.
2. Koblitz, N., 1987. Elliptic Curve Cryptosystems, Math. Comput., 48: 203-209.
3. Miller, V., 1986. Uses of Elliptic Curves in Cryptography, Advances in Cryptology, proceedings of Cryto’ 85, pp: 417-426.
4. Sivavakeesar, S., G. Pavlou, C. Bohoris and A. Liotta, 2004. Effective management through prediction-based clustering approach in the next-generation ad hoc networks, IEEE Commun. Soc., 7: 4326-4330.
5. Yan Lindsay Sun, Wei Yu, Zhu Han and K.J. Ray Liu, 2006. Information theoretic framework of trust modeling and evaluation for ad hoc networks, IEEE J. Selected Areas in commun., 24: 305-317.
6. Payman Arabshahi andrew Gray, Ioannis Kassabalidis and Arindam Das, 2001. Adaptive Routing in Wireless Communication Networks using Swarm ntelligence International Communications Satellite Systems Conference, pp: 17-20, 2001.
7. Qiang Huang, Johnas Cukier, Hisashi Kobayashi, Bede Liu and Jinyun Zhang, 2003. Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks, in Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pp: 141-150.
8. Tikiner, F., Z. Ghassemlooy and S. Al-Khayatt, 2004. Improved Routing Algorithm with link probability evaporation over the given time window, IEEE SoftCOM2004, pp: 11- 13.
9. Jiang, M., J. Li and Y.C. Tay, 1999. Cluster Based Routing Protocol (CBRP) Function Specifications, IETF Draft.
10. Rohatgi, P., 1999. A compact and fast hybrid signature scheme for multicast packet authentication, in ACM Conference on Computer and Communications Security.