TARP: Trust-Aware Routing Protocol

L. Abusalah, A. Khokhar
Department of Electrical and Computer Engineering
University of Illinois at Chicago, USA
{labusa1, ashfaq}@uic.edu

G. BenBrahim, W. ElHajj
Department of Computer Science
Western Michigan University Kalamazoo, MI, USA
{benbrahim,welhajj}@cs.wmich.edu

ABSTRACT
Security is a critical issue in a mobile ad hoc network (MANET). In most of the previous protocols security is an added layer above the routing protocol. We propose a Trust-Aware Routing Protocol (TARP) for secure-trusted routing in mobile ad hoc networks. In TARP, security is inherently built into the routing protocol where each node evaluates the trust level of its neighbors based on a set of attributes and determines the route based on these attributes. This paper evaluates the proposed TARP protocols on two important attributes, the *battery power* and the *software configuration*. A secure route between a source and destination is established based on a confidence level prescribed by a user or application in terms of these attributes. Our performance evaluation shows that TARP is a robust and adaptive trust routing algorithm that reacts quickly and effectively to the dynamics of the network while still finding the shortest path to the destination. TARP is able to improve security and at the same time reduce the total routing traffic sent and received in the network by directing the traffic based on the requested sender attributes.

Categories and Subject Descriptors
C.2.1 Network Architecture and Design (*Wireless communication)*.

General Terms
Security, Reliability, Performance, Design.

Keywords
Ad Hoc, Trust, Power, Encryption, Aware Routing.

1. INTRODUCTION
An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration [1]. The absence of any central coordination or base station makes the routing complex when compared with regular cellular networks.

Several protocols have been introduced for Ad Hoc routing. The issues related to the design of the ad hoc routing protocols are inherently related to the ad hoc application. Routing protocols are designed for purposes such as quality of service provisioning, energy management and security.

IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada.

A noteworthy on-demand protocol called Dynamic Source Routing (DSR) protocol was developed by Johnson *et al.* [2]. DSR was designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table update messages required in the proactive routing protocols.

The problem of routing was divided into two areas - route discovery and route maintenance. In order for one host to communicate with another, it must initially discover a suitable route to use in sending packets to that destination. As long as conditions remain unchanged, this route should be maintained as long as it is needed.

Many secure versions such as QoS [3], SQoS [4], Ariadne [5] and CONFIDANT [6] have been developed from the basic design of DSR. The process of identifying routes based on the trust level of nodes has not been addressed in such previous work [3-10]. Also, the major issue is to determine the trust metric based on a given set of parameters/attributes.

A secure ad hoc network has to meet different security requirements [11]:

Confidentiality: Data which has been transmitted should only be interpreted by the intended receiver. To meet this requirement data encryption is used.

Integrity: Data should not change during the process of sending. Data integrity must be ensured.

Availability: Network services should be available all the time and it should be possible to correct failures to keep the connection stable. However, the level of trust that may be associated with each available route should be determined and advertised to the user.

Most of the existing research work [3-10, 16-17] focuses on confidentiality and integrity. TARP will focus more on the availability as an important factor in securing ad hoc networks. The proposed protocol has been simulated using OPNET [15] for two important attributes, the battery power and the software configuration. The results show that TARP is able to improve network availability and reduce the routing traffic sent and received by 37.7% and more than 70%, respectively, while still maintaining an acceptable route discovery time and an acceptable delay.

The rest of this paper is organized as follows: Section II describes the novel Trust Aware Routing Protocol (TARP). The battery power and the software configuration attributes will be discussed in detail. Section III analyzes the performance of TARP through simulations and Section IV concludes the paper.

2. TRUST AWARE ROUTING PROTOCOL
TARP selects routes to the destination based not only on the shortest path but also on several other security oriented attributes of the nodes. Only nodes that match the sender requirements would forward the packet. The main objectives of

the proposed TARP suite are: (a) implement security that is inherently built into the routing protocol, (b) deliver messages that are received with a user defined or best available level of confidence, (c) allow users and applications to prescribe their required level of security, (d) achieve efficiency in routing that is improved by limiting control message exchanges, (e) optimize resource usage, (f) obtain graceful network performance degradation, and (g) develop a protocol suite that adapts to changes in the environment, such as the network topology, the power-level of nodes, etc.

In TARP, the security parameters considered in computing the trust-level of a node in a given route include: *software configuration*, *hardware configuration*, *battery power*, *credit history*, *exposure* and *organizational hierarchy*. Each node evaluates the trust level of its neighbors based on the above parameters and includes it in computing the next hop node in the overall shortest route computation. Due to page limitations, this paper will focus on the implementation and evaluation of the battery power and the software configuration attributes. Below is a description of the battery power and software configuration attributes:

- Power: In wireless networks, the battery power with which nodes operate is a limited resource. Each node uses its power to not only send and receive, it also behaves as a router by forwarding routing messages and updates. The cryptographic techniques that provide security are computationally intensive, which further increase the power consumption of a node. The node's trust level should be set to low since it cannot guarantee its service. This illustrates that power is an important parameter for evaluating the trust level of a node.
- Software Configuration: The software configuration includes the encryption ability of a node. To satisfy CAI (Confidentiality, Availability and Integrity), different cryptographic mechanisms have been proposed. Some are based on symmetric encryption and others on asymmetric encryption. Each node is given either a shared secret key or a public/private key pair depending on the type of cryptographic mechanism. Different encryption algorithms are available such as RSA, DES/3DES, BLOWFISH, IDEA, SEAL RC2/RC4/RC5/RC6 [12]. Strong encryption is often discerned by the key length used by the algorithm. In general, a node with a stronger encryption algorithm has a higher trust level than a node with a weaker encryption algorithm.

2.1 Battery Power

We will adopt the DSR mechanism in finding the shortest path to the destination. However, DSR does not take into consideration the node power factor. We will modify the packet format for the RouteRequest in the Route discovery mechanism to carry additional two bits, which will allow the sender to choose among four levels of power: LOW, MID, HIGH, V.HIGH. Fig. 1 shows TARP RouteRequest Packet Format.

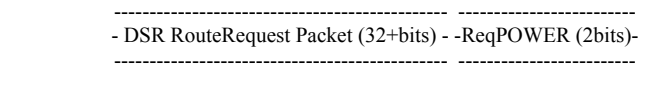

Figure 1. Power TARP Packet Format.

If node S wishes to communicate with node D, it needs to find a route on demand by using a route discovery mechanism. Node S broadcasts a RouteRequest packet in the network. This RouteRequest contains the address of the initiator, the address of the target, a field sequence number (sets the initiator and used to identify the request) and a route record (where a record of the sequence of hops taken by the RouteRequest is accumulated dynamically). Each node in the network maintains a table in order to detect a duplicate RouteRequest packet received. A node propagates the RouteRequest if (i) the intermediate node is not the target, (ii) it is not the first time it receives this packet and (iii) if its power is greater than or equal to the sender ReqPower.

The first node receiving this request that has a valid route in its route cache for node D initiates a Route Reply packet back to node S. This Route Reply contains the list of nodes along the path from node S to node D. (Route cache entries will maintain one half the time required for regular DSR, because the node power is changing by time). The first part is the information gathered along the path of the RouteRequest (that is, from node S to the node replying); the rest of the list is the information found in the route cache of the replying node. Moreover, it may occur that destination node D itself receives a RouteRequest packet, e.g., no node along the way before node D has an accurate route from node S to node D in its route cache. In this case, node D sends a RouteReply packet containing the path just created dynamically from source S to destination D, i.e., the path traversed by the first RouteRequest packet received by node D. This path is the minimum delay route from node S to node D. Node D discards all RouteRequest packets corresponding to the same route discovery process after the arriving of the first one.

The route maintenance ensures that the paths stored in the route cache are valid. If the data link layer of a node detects a transmission error, the uplink node creates a RouteError packet and transmits it to the original sender of the data packet. This RouteError packet indicates which link is broken, i.e., the node that detected the error and the node it was trying to reach. When a node receives a RouteError packet, it removes the link in error from its route cache and for each route containing this link, truncates the route from the hop before the broken link. TARP ignores the ReqPOWER in the route maintenance procedure. However, the requested power will be considered in the next scheduled transmission.

In order to have feedback on the status of each node, several acknowledgement mechanisms may be used, e.g., ACK at the MAC layer level, request of an explicit ACK from the next-hop receiver in the data packet header, or passive ACK (that is, a node overhears the next node forwarding its packets). In Fig. 2, the source node is node 1 and the destination node is node 15. Node 1 will send a RouteRequest to all its neighbors 2, 5 and 6. Node 1 is requesting HIGHPower for its transmission. Each node receiving this request will read the ReqPower (found on the sender RouteRequest field of the packet) and compare it to its current power level.

In this example, only node 2 will forward the message. The same procedure will be performed by nodes 2, 4, 8, 13 and 15. A route reply will take the same route (the destination node, node 15, has also the option to do a route discovery based on the sender ReqPower). If the link between nodes 8 and 13 is unavailable, (see Fig. 3) because node 13 may have shut down or relocated, then node 8 will start a timer and will try to find a PowerRoute to the destination. If node 8 does not find a

PowerRoute, it will establish a NONE PowerRoute. However, this path will not be selected the next time the sender initiates a Route Discovery. If there is no PowerRoute to the Destination, the sender will get a message indicating a route error because of the ReqPower.

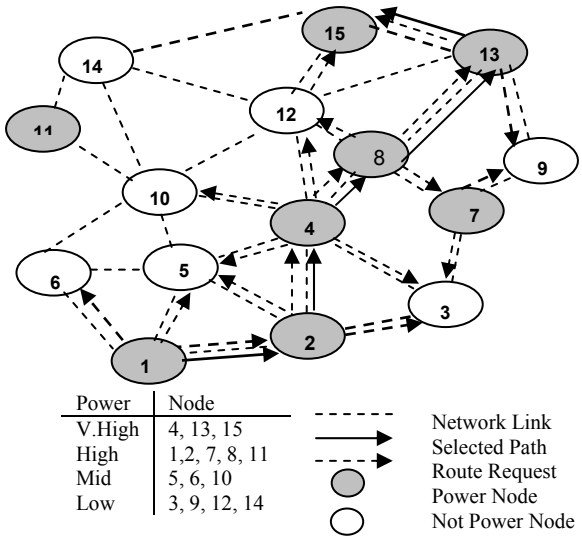

Figure 2. Route Discovery in Power TARP.

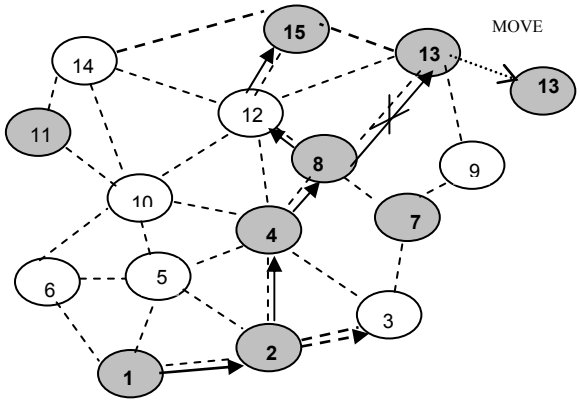

Figure 3. Route Maintenance in Power TARP.

2.2 Software Configuration

Data will be distributed among a variety of mobile devices, such as laptops, personal digital assistants (PDAs), mobile phones, in-vehicle computer systems, etc. Different secure ad hoc routing protocols might exist in any ad hoc network and the sender should have the right to choose which secure route he might utilize to send data or the sender might choose not to have any security requirements.

We will modify the packet format for the RouteRequest in the Route discovery mechanism to carry an additional two bits, in which it will give the sender the chance to select among four encryption mechanisms NONE, Encry1, Encry2 and Encry3 (Encry1, Encry2 and Encry3 could be one of the following: RSA, DES/3DES, BLOWFISH, IDEA, SEAL RC2/RC4/RC5/RC6).

Fig. 4 shows the Route Discovery in Encrypted TARP. The sender, node 1, will initiate a RouteRequest to the destination, node 15 asking for Encry1. Nodes 2, 5 and 6 will get the RouteRequest. All the nodes will compare their Encryption mechanism to the Requested Encryption by reading the encryption field in the RouteRequest. Node 5 is the only one which matches the Requested Encryption.

Only Node 5 will forward the RouteRequest to all its neighbors. Nodes 10, 12 and 14 will do the same. Node 15 will respond only to the first RouteRequest. If the RouteRequest through node 14 is the first to reach the destination, then 1-5-10-14-15 route will be selected for forwarding the packets and the connection will be established.

If node 14 moves away or shuts down, the uplink node (10) will be responsible for finding another secure route to the destination. Node 10 will set a timer, and start the route maintenance procedure

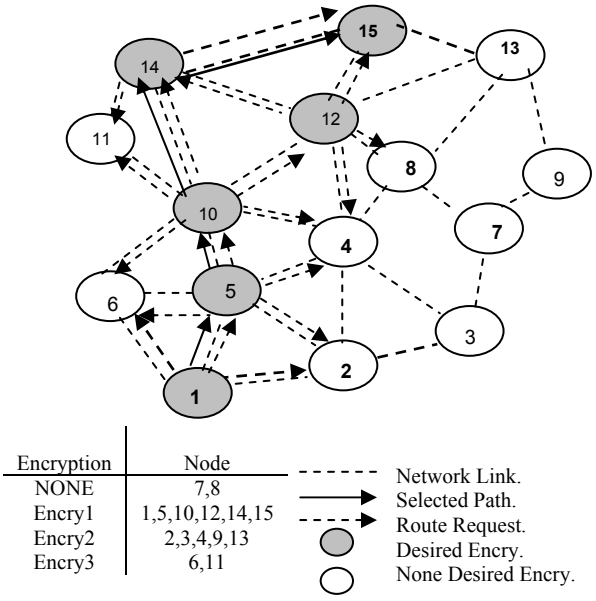

Figure 4. Route Discovery in Encrypted TARP.

in finding the secure route. In this example, the alternative way is through node 12. The new route will then be established. If node 12 fails to establish a route to the destination then it will send back an error message to the sender. The sender will then have the choice to retry and find a secure route with the same encryption criteria or may change to a different one. Power TARP and Encrypted TARP can work together to form a strong trusted routing protocol. The sender can specify the amount of power and the type of encryption for the transmission.

3. PERFORMANCE EVALUATION

TARP has its own algorithm to find a secure route to the destination based on three factors: (a) the shortest stable route to the destination, (b) the requested sender power, and (c) the requested sender type of encryption.

We have evaluated the performance of TARP on DSR via simulation using OPNET [15]. To assess the performance of TARP, we studied the battery power attribute represented by Power TARP and then the software configuration attribute represented by Encrypted TARP. By choosing different scenarios, we were able to study both stationary and mobile

node networks with different scales. For the stationary network we have chosen three different scenarios, using 25, 50 and 100 nodes. The nodes run an FTP session randomly. For the mobile network, we have chosen two scenarios using 25 and 50 nodes. Each node sends a message to any arbitrary node. We run each simulation 50 times on the average.

3.1 Power TARP

Power TARP is based on selecting a secure route based on the sender requested power choice. The first scenario is a stationary network. Table I shows the simulation configuration. Fig. 5 shows the routing traffic sent for a 25 stationary nodes compared to DSR. The routing traffic sent by DSR for 25 workstations is 71.2 bits/sec, while the routing traffic sent by the same network using TARP with 5 stations requesting HIGHPower is 56.8 bits/sec, which shows a 20.2 % improvement. The routing traffic sent for TARP with 10 stations requesting HIGHPower is 53 bits/sec, which is a 25.5% improvement.

Fig. 6 shows the routing traffic received for 25 stationary nodes. The routing traffic received by DSR is 95.9 bits/sec, while the routing traffic received by the same network using TARP with 5 stations requesting HIGHPower is 80.3 bits/sec, which is 16.3 % better. The routing traffic received by TARP with 10 stations requesting HIGHPower is 80.64 bits/sec, which 16% better.

Table I. Simulation Configuration

Category	Value
Application	FTP
Station operation mode	Serial (ordered)
start time (sec)	100
Duration	End of Simulation
stations transmission range (m)	1500
Avg. distance between stations (m)	1000

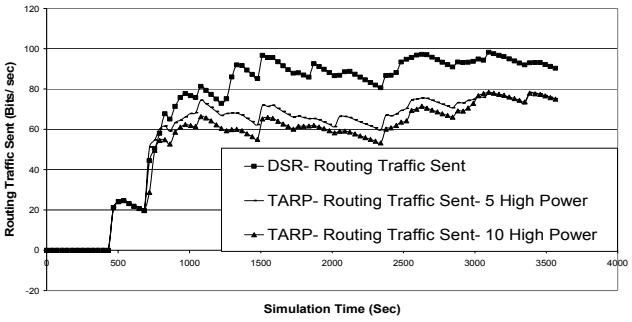

Figure 5. Routing Traffic Sent for Power TARP.

The route discovery time has also been reduced when the number of nodes requesting HIGHPower have at least double the number of nodes with HIGHPower, i.e., the number of total nodes is 25, 10 at least with high power, 5 out of the 10 are requesting HIGHPower. The results show that Power TARP 5-10-25 (5 Requesting HIGHPower-10 with HIGHPower- 25 is the total number of nodes) has improved the route discovery time by 1ms. However, in Power TARP 10-10-25 the route discovery time has increased as expected by 3ms in the beginning of the simulation. By the end of the simulation the route discovery time was close to DSR.

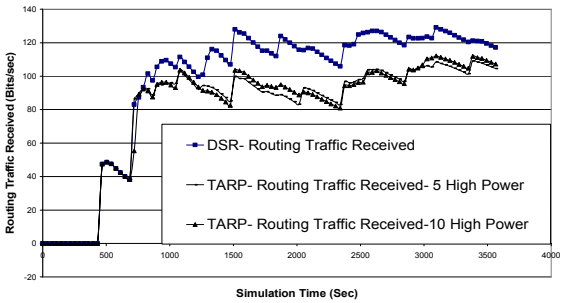

Figure 6. Routing Traffic Received in Power TARP.

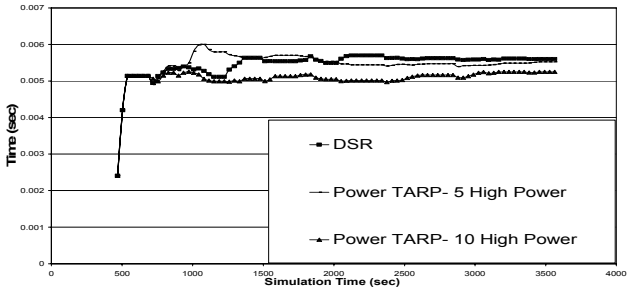

Figure 7. Overall network delay.

The delay in the network, as depicted in Fig. 7, has also been reduced by 0.5 ms for Power TARP 5-10-25 and by 1ms for Power TARP 10-10-25. The delay represents the end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer. This delay includes medium access delay as the source MAC and the reception of all fragments individually.

Table II shows the simulation results for 50 and 100 node networks. In a 50 node network, two scenarios have been chosen. The first is 10-25-50, with 10 nodes requesting HIGHPower, 25 with HIGHPower and the total number of nodes in the network is 50. The second scenario is 25-25-50.

Table II
Power TARP Simulation Results for 50 and 100 Node Network

100	Scenario/Protocol		Protocol/Scenario	**50**
953	DSR	RTS (bits/ sec)	DSR	199
837	20-50-100/PTARP		PTARP/ 10-25-50	197
733	50-50-100/PTARP		PTARP/ 25-25-50	176
1392	DSR	RTR (bits/ sec)	DSR	278
1317	20-50-100/PTARP		PTARP/ 10-25-50	273
1145	50-50-100/PTARP		PTARP/ 25-25-50	258
7.3	DSR	RDT (ms)	DSR	0.009
7.6	20-50-100/PTARP		PTARP/ 10-25-50	0.009
7.2	50-50-100/PTARP		PTARP/ 25-25-50	0.011
5.0	DSR	Delay (ms)	DSR	0.464
5.0	20-50-100/PTARP		PTARP/ 10-25-50	0.463
7.17	50-50-100/PTARP		PTARP/ 25-25-50	0.467

RTS: Routing Traffic Sent RDT: Route Discovery Time
CTS: Routing Traffic Received PTARP: Power TARP
10-25-50: 10 Requesting HIGHPower, 25 Having HIGHPower, 50 total Number of Nodes

Also, two scenarios have been chosen in the 100 node network, the first is 20-50-100 and 50-50-100. We notice that the routing traffic sent or received is always less than or equal to the routing traffic sent or received in DSR. On the other hand, the route discovery time and the delay in the network is either equal to DSR or more than DSR by not more than 20%. This is expected for two reasons: (1) the RouteRequest packet has been increased two bits; (2) the node will take more time to check the requested power. This is the tradeoff for adding a secure attribute.

3.2 ENCRYPTED TARP

Encrypted TARP is based on selecting a secure route based on the sender requested encryption choice. We built the Encrypted TARP on Power TARP. Fig. 8 shows the routing traffic sent and received by two scenarios. The first scenario is where all the nodes are communicating based on the same power and no encryption is requested by the senders. The second scenario' based on 15 nodes with "Encryption 1", 5 nodes with "Encryption 2" and 5 nodes with "Encryption 3". Only 5 nodes request "Encryption 1". All other nodes request no encryption. The results show a 17% improvement in the routing traffic sent and a 5% improvement in the routing traffic received. Further improvement may be achieved if the number of nodes with "Encryption 1" decrease (fewer nodes involve in routing).

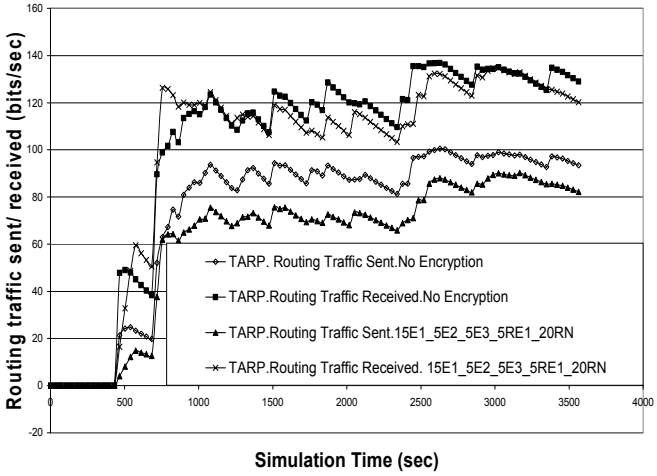

Figure 8. Routing Traffic Sent/ Received for Encrypted-Powered TARP.

The wireless delay in Fig. 9 also has improved by 1ms. The route discovery time has increased additional 10ms. Again, this is an expected tradeoff between security and time.

3.3 Large Scale Networks

The simulation results for 50 and 100 nodes Ad hoc networks are shown in Table III. The routing traffic sent for 50 nodes shows improvement by 37.7% and a 70% improvement in the routing traffic received. However, the average route discovery time has increased by 4.4ms and the delay has increased by 0.5 ms.

The routing traffic sent and received for 100 nodes shows improvement by more than 100%. On the other hand and as a tradeoff, the route discovery time has increased 6.2 ms with a 1.3 ms increase in the delay.

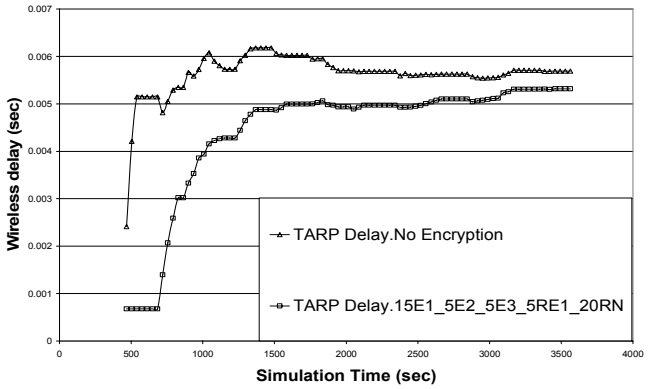

Figure. 9 Delay for Encrypted Powered TARP.

Table III
EP-TARP Simulation Results for 50 and 100 Node network.

100	Scenario/ Protocol		Protocol/ Scenario	**50**
200.2	25-0-100/ DSR	RTS (bits/ sec)	DSR/ 7-0-50*	47.7
88.0	25-25-100/ EP-TARP		EPTARP/ 7-7-50	29.7
321.6	25-0—100/ DSR	RTR (bits/ sec)	DSR/ 7-0-50	115
134.32	25-25-100/ EP-TARP		EPTARP/ 7-7-50	34.56
9.8	25-0-100/ DSR	RDT (ms)	DSR/ 7-0-50	10.2
16.0	25-25-100/ EP-TARP		EPTARP/ 7-7-50	14.6
4.3	25-0-100/ DSR	Delay (ms)	DSR/ 7-0-50	3.6
5.6	25-25-100/ EP-TARP		EPTARP/ 7-7-50	4.1

RTS: Routing Traffic Sent RDT: Route Discovery Time
CTS: Routing Traffic Received EP-TARP: Encrypted Power TARP
* 7-0-50: 7 nodes sending packets, 0 nodes asking for special encryption, 50 total nodes.

3.4 Mobility

Mobility ad hoc networks are implemented for 25 and 50 nodes. However, the mobility will not affect Power TARP (compared to DSR) because route maintenance does not take the ReqPower into consideration. Fig. 10 shows that the Routing Traffic sent and received for Power TARP with 5 nodes requesting HIGHPower is almost identical with DSR.

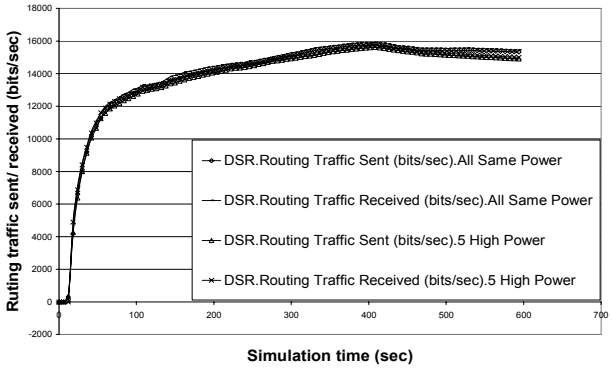

Figure 10. Routing Traffic send and received for 25 mobile ad-hoc nodes in Power TARP.

The requested encryption will be considered in the TARP maintenance procedure. Fig. 11 shows that the routing traffic sent and received by TARP 15E1_5E2_5E3_5RE1_20RN (15 nodes with "Encryption 1", 5 nodes with "Encryption 2", 5 nodes with "Encryption 3", 5 nodes "Requesting Encryption 1" and 20 " Requesting No encryption") is almost identical to DSR.

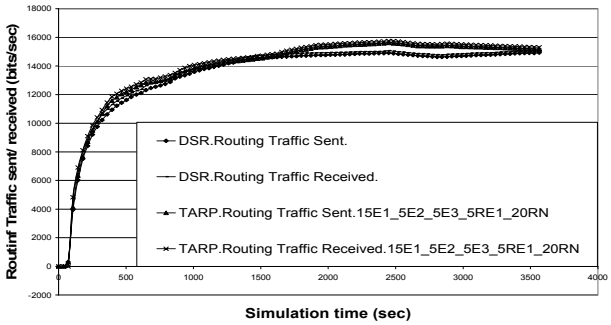

Figure 11. Routing traffic send and received for 25 mobile ad hoc nodes in Encrypted TARP.

Table IV shows the route discovery time for DSR, Power TARP and Encrypted TARP in two scenarios, 25 and 50 nodes. In the 25 node network, the results show that the route discovery time has increased 0.8s and 1.1s for Power TARP and Encrypted TARP, respectively.
In the 50 node network, the results show that the route discovery time has increased 0.9s and 3.7s for Power TARP and Encrypted TARP, respectively. This tradeoff is considered acceptable for a high mobility large networks with limited resources.

Table IV
Route Discovery Time comparison for 25 and 50 Mobile Node Ad Hoc Network.

# of Nodes	Type	Route Discovery Time (s)
25	DSR	0.6
	Power TARP	1.4
	Encrypted TARP	1.7
50	DSR	6.7
	Power TARP	7.6
	Encrypted TARP	10.4

4. CONCLUSIONS

This paper has presented and evaluated TARP as a new novel routing scheme focusing on network availability. TARP can be implemented to protocols such as DSR [2], AODV [14], Ariadne [5] and SAODV [17]. The major issue is to determine the trust metric based on a given set of parameters. The results of implementing the software configuration and the battery power have been presented. Different scenarios, such as stationary and mobile nodes, have been used to analyze TARP on networks with 25, 50 and 100 nodes. The study shows that TARP is able to improve the security of an ad hoc network as well as reduce the routing traffic, while still maintaining an acceptable route discovery time and an acceptable delay. The routing traffic is directly related to the number of nodes that meet the sender's requirements. In our future work, we plan to combine the effects of different trust attributes into one trust metric and evaluate the performance of TARP based on the collective metric.

5. REFERENCE

[1] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols," *Prentice Hall*, Chapter 7, 1994.

[2] D. B. Johnson and D. A. Maltz, "Dynamic Sources Routing in ad Hoc Wireless Networks," *Mobile Computing*, 1996

[3] Don Coppersmith and Markus Jakobsson, "Almost Hash Sequence Traversal," In proceeding of the Fourth Conference on Financial Cryptography (FC '02), Lecture Notes in computer Science, 2002.

[4] Yih-Chun Hu and D. B. Johonson, "Securing Quality-of-Service Route Discovery in On-Demand Routing for Ad Hoc Networks," *Proceedings of ACM SASN '04*, October 20, 2004.

[5] Yih-Chun Hu, A. Perrig, and D. B. Johonson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proceedings of ACM MobiCom '02*, September 23-26, 2002.

[6] S. Buchegger and Jean-Yves Le Boudec, "Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes—Fairness In Dynamic Ad-hoc Networks," *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, 2002.

[7] W. Lou and W. Liu, and Y. Fang, "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks," *Proceedings of IEEE INFOCOM 2004*, 2004.

[8] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," *Proceedings of IEEE Network Protocols, 2002*, pp. 78-87, November 12-515, 2002.

[9] S. Yi, P. Naldurg, and R. Kravets, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks," *Proceedings of ACM MobiHoc '01*, 2001.

[10] Yih-Chun Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *Proceedings of IEEE Mobile Computing Systems and Applications, 2002*, pp. 3-13, 2002.

[11] D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*, 1995.

[12] A. Murat Fiskiran and Ruby B. Lee, "Performance Impact of Addressing Modes of Encryption Algorithms," IEEE International Conference on Computer Design (ICCD'01), pp. 542- 545, 2001.

[13] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *Proceedings of IEEE INFOCOM '97*, pp. 1405-1413, 1997.

[14] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," *Proceedings of 2nd IEEE Workshop Mobile Computer Systems and Applications*, pp. 90-100, 1999.

[15] OPNETUniversityProgram: http://www.opnet.com/services/university/

[16] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks," *IFIP-Communicatin and Multimedia Securtiy Conference 2002.*

[17] M. Guerrero Zapata, "Secure Ad hoc On-Demand Distance Vector Routing," *Mobile Computing and Communications Review*, vol. 6, no. 3.