Performance Enhancement with Multipath Routing in Term of Bandwidth and Security on MANETs

Sandhya Umrao
Professor in Department of Information & Technology
Galgotiya's College of Engineering and Technology, Greater Noida, India

Rajneesh Gujral, PhD
Professor in Department of computer science & Engineering
M.M.U. Mullana, Ambala, India

ABSTRACT
In Mobile Ad hoc Networks (MANETs) providing performance enhancement in term of bandwidth, security for soft real time processing services is very difficult. All routing protocols are intended for operation in a trusted environment in which all nodes are honest, and they do not consider the disruptions that can be caused by a malicious attacker sending arbitrary (e.g. forged) routing packets. In this paper, we have proposed a performance enhancement with multipath routing in term of bandwidth and security on MANETs that reactively collects link-state information from source to destination in order to dynamically construct a flow network. The QoS enabled multipath routes between source and destination has been detected by destination node under the CDMA-over-TDMA channel model of MAC layer, which collectively satisfy required bandwidth and security services during route discovery process. For secure route discovery, we use hashing chain and onion encryption an asymmetric key cryptography for authenticating source to destination route, so that no modification is done during en-route process.

Keywords
Multipath routing, QoS, bandwidth, security etc.

1. INTRODUCTION
In ad hoc wireless networks, the QoS requirements are more influenced by the resources of the nodes, some of the resource constraints are battery charge, processing power and buffer space. The goal of QoS provisioning is to achieve a more deterministic network behaviors, so that information carried by the network can be better delivered and network resources can be better utilized[1]. The QoS parameters differ from application to application e.g., in case of multimedia application bandwidth, delay jitter and delay are the key QoS parameters, where military applications have stringent security requirements. For applications such as emergency search-and-rescue operations, availability of the network is the key parameter. Applications such as group communication in a conference hall require that the transmission among nodes consume as little energy as possible. Hence, battery life is the key QoS parameter here.

In QoS routing, after receiving a QoS service request from the user, the first task is to find a suitable loop-free path from source to destination having necessary resource available to meet the QoS requirements of the desired service. As shown in table 1, the attributes of each link in the network are shown as a tuple $< \mathrm{Bw}, \mathrm{D} >$, where Bw and D represent available bandwidth in Mbps and delay in ms. Suppose a packet from node B to G requires a bandwidth guarantee of 4 Mbps. Table 8.1 demonstrates that six paths are available between B and G in the existing network. QoS routing selects path 3 $i.e.(B,C,F,G)$ because this is the only path that meets the bandwidth constraints.

Table 1. Available Paths from node B to G

No.	Path	Hop Count	End-to-end Bandwidth (Mbps)	End-to-end Delay (milliseconds)
1	B → E → G	2	2	9
2	B → E → F → G	3	2	11
3	B → C → F → G	3	4	15
4	B → C → F → E → G	4	3	19
5	B → A → D → E → G	4	2	23
6	B → A → D → E → F → G	5	2	25

The increase in multimedia, military application traffic has led to extensive research focused on achieving guaranteed QoS enabled communication in term of security and bandwidth over MANETs. The previous research work is not so much concentrated on providing both security and bandwidth for QoS provisioning in MANETs.

S. Chen et al. [2] proposed a distributed, QoS routing protocol that uses tickets to find delay-constrained or bandwidth-constrained routes. Tickets are distributed during route discovery to provide a means to find routes with available bandwidth/delay and limit the flooding for route request packets. Resource estimation is required in ticket-based QoS routing to enable each node to determine the delay, bandwidth, and cost of each of its links. Ticket-based QoS routing assumes that this bandwidth/delay information can be obtained from lower layers. AOMDV [3] offers a multipath, loop-free extension to AODV. It ensures that alternate paths at every node are disjoint, therefore achieves path disjointness without using source routing. To support multipath routing, route tables in AOMDV contain a list of paths for each destination. All paths to a destination have same destination sequence number. Once a route advertisement with a higher sequence number is received, all routes with the old sequence number are removed. Two additional fields, hop count and last hop, are stored in the route entry to resolve the problems of loop freedom and path disjointness.

Split Multipath Routing (SMR) [4] is a multipath version of DSR. Unlike many prior multipath routing protocols, which keep multiple paths as backups routes, SMR is designed to

utilize multipath concurrently by splitting traffic onto two maximally disjoint routes. Two routes said to be maximally disjoint, if the number of common links are minimum. De et al. [5] proposed a Trigger-based on-demand Distributed QoS Routing (TDR) protocol for supporting real-time applications in ad hoc wireless networks. This protocol differs from other location-based protocols due to the use of a local neighborhood database during route discovery, soft reservations, and route break prediction to support QoS. TDR assumes that bandwidth estimation is performed in lower layers. In [6], a reactive routing protocol based on AODV called Bandwidth Estimation QoS Routing (BEQR) is proposed that incorporates adaptive feedback and admission control by estimating the available bandwidth at each host during route discovery. BEQR supports both call admission and adaptive feedback to the source node.

Y. Hwang et al. [7] proposed an algorithm to find multiple disjoint routes with long lifetimes and it differs from other QoS routing protocols in terms of using signal strength as a parameter to predict route breaks and initiate a fast reroute of data. Information on the estimated bandwidth is assumed to be obtained from lower layers. Core-Extraction Distributed Ad hoc Routing (CEDAR) [8] is a routing protocol that dynamically establishes a core set for route set up, QoS provisioning, routing data, and route maintenance. A greedy algorithm is used to proactively create an approximate minimum dominating set, whereby all hosts in the network are either members of the core or one-hop neighbors of core hosts. Only core hosts maintain local topology information, participate in the exchange of topology and available bandwidth information, and perform route discovery, route maintenance, and call admission on behalf of these nodes. Lin et al. [9] proposed an admission control scheme over an on-demand QoS routing (OQR) protocol to guarantee bandwidth for real-time applications. Since routing is on-demand in nature, there is no need to exchange control information periodically and maintain routing tables at each node. Similar to Bandwidth Routing (BR) protocol, the network is time-slotted and bandwidth is the key QoS parameter. On-demand Node-Disjoint Multipath Routing protocol (NDMR) is another protocol that allows the establishment of multiple paths between a single source and destination node [10].

A Swarm Intelligent Multipath routing for multimedia traffic over MANETs was proposed to predict the significant traffic problems such as packet losses, transmission delayed, delay variation etc. in real time [11]. A Multipath Routing protocol for ad hoc network called "Predicted Multipath Routing Protocol (PMP)" [12] generates a set of disjointed paths having well-enough availability and high performance. The strategy of selecting path, qualifying the requirements depends on two measurements: The degree of availability (DA) and the estimated path throughput value (ETV). The DA relies on potential signal strength, which is affected by mobility of nodes in the network. The ETV engages with the packet loss ratio that can scale efficiency of a path. A self-authentication based secure routing protocol; called "Secured Predictive Multipath Routing Protocol (SPMP)" [12] consists of three phases: the first phase is associated with authentication process, enabling a pair of nodes to compromise their trust. The second phase is concerned with on-demand route discovery. The last phase incorporates key exchange infrastructure in order to maintain end-to-end data secrecy.

2. ROUTING SECURITY ISSUES AND THEIR EXISTING SOLUTION

The basic security services are Authentication, Confidentiality, Integrity and Availability. The goal of these services is to protect information and resources from attacks. If routing protocol is subverted and messages are altered in transit, then security at upper layers cannot mitigate threats. In Table 2 and Table 3, we review the attacks and existing solutions for reactive routing protocol DSR and AODV.

Table 2. Attacks on DSR and AODV Protocols

Attack	AODV	DSR
Attacks using modification	Yes	Yes
Modifying route sequence numbers	Yes	No
Modifying hop counts	Yes	No
Modifying source route	No	Yes
Tunneling	Yes	Yes
Spoofing attacks	Yes	Yes
Falsifying route errors	Yes	Yes
Broadcast falsified routes	No	Yes
Rushing attacks	Yes	Yes

Table 3. Secure Routing Solutions For DSR And AODV

Solutions	Attacks Prevented	Drawbacks
Authentication during all phases	All external attacks, and internal attacks Spoofing Redirection by modifying route sequence number	Requires certificate authority or key sharing mechanism
Trust-level metric	All attacks prevented by authentication All attacks on higher trust-level nodes	Requires certificate authority or key sharing mechanism. Difficulty in defining trust level
Secure neighbor verification	All attacks prevented by authentication Rushing	Requires certificate authority or key sharing mechanism. More overhead when mobility increases
Randomize message forwarding	Rushing	Latency

The above solutions can be classified in the following categories; solutions based on asymmetric cryptography, solutions based on symmetric cryptography, hybrid solutions and reputation-based. In this paper we use hash chaining and asymmetric key cryptography (onion encryption) to preserve the security in routing process.

3. PROPOSED MULTIPATH ROUTING PROTOCOL FOR PERFORMANCE ENHANCEMENT

Multipath routing is a technique that exploits the underlying physical network resources by utilising multiple source-destination paths. It is used for various purposes including bandwidth aggregation, minimizing end to end delay, increasing fault-tolerance, enhancing reliability and proper load balancing. The proposed protocol searches for multiple paths which collectively satisfy the required bandwidth requirement X. The original bandwidth requirement is split in to sub-bandwidth requirements. A mobile node in the

network knows the bandwidth available to each of its neighbors. When source node requires a QoS session with bandwidth X to destination node, it floods QRREQ (QoS Route Request) packet in the network.

Source node S floods a QRREQ $\{S_{id}, D_{id}, N_h = \{S\}, F_{ts} = \{\phi\}, X, TTL\}$ packet in the network toward the destination D. If the given bandwidth requirement is X then all intermediate nodes receiving a QRREQ packet will perform any of the following events:

Event 1: Node N checks the node history N_h field of the QRREQ packet for its address. If it exists, then N will discards this QRREQ packet.

Event 2: Node N decrements TTL by one and if TTL counts becomes zero, the QRREQ packet is discarded. Otherwise, N adds itself into the node history field, appends the free time-slots of the link between itself and the last node recorded in the node history field into the list of free time-slots and then rebroadcasts this QRREQ packet. Destination eventually receives many different QRREQ packets from source. Destination will re-configure the network topology on the basis of free time-slot information.

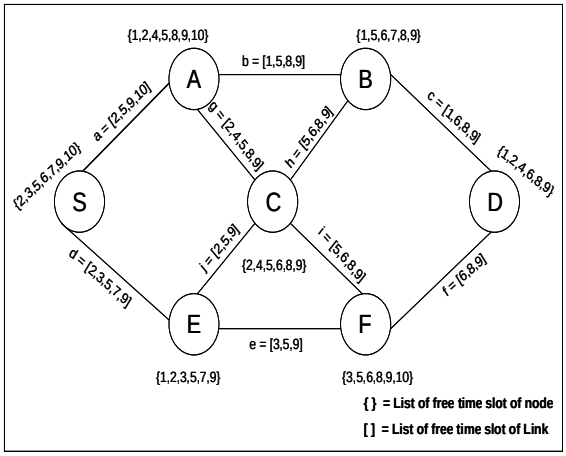

Fig 1: Ad hoc Network Topology

For the network as shown in Figure 1, the following six QRREQ packets are received at destination D from source S through different routes:

1. QRREQ $\{S, D, \{S, A, B, D\}, [2,5,9,10], [1,5,8,9], [1,6,8,9], X, TTL\}$
2. QRREQ $\{S, D, \{S, E, F, D\}, [2,3,5,7,9], [3,5,9], [6,8,9], X, TTL\}$
3. QRREQ $\{S, D, \{S, A, C, B, D\}, [2,5,9,10], [2,4,5,8,9], [5,6,8,9], [1,6,8,9], X, TTL\}$
4. QRREQ $\{S, D, \{S, A, C, F, D\}, [2,5,9,10], [2,4,5,8,9], [5,6,8,9], [6,8,9], X, TTL\}$
5. QRREQ $\{S, D, \{S, E, C, B, D\}, [2,3,5,7,9], [2,5,9], [5,6,8,9], [1,6,8,9], X, TTL\}$
6. QRREQ $\{S, D, \{S, E, C, F, D\}, [2,3,5,7,9], [2,5,9], [5,6,8,9], [6,8,9], X, TTL\}$

To embed security during route discovery process, the main challenge is to ensure that each intermediate node cannot remove or add extra node in the node history (N_h) field of QRREP packet. The following QRREQ messages are routed from source S to destination D for path (S, A, B, D).

Step1: Source S generates $P_S = (QRREQ, S, D, X, TTL)$

Step2: To authenticate the contents in the chain, the intermediate node A calculate h_A i.e. hash of (P_S, A) with hashing algorithm. H And to authenticate source - destination relation, it generates chain of hash codes. So far, node A generated P_A and broadcasted it locally. This process is followed by all the intermediates node of given path (S, A, B, D) in the following manner:

S : $P_S = (QRREQ, S, D, X, TTL)$

$S \rightarrow *: (P_S)$

A : $h_A = H(A)$,

$P_A = (QRREQ, S, D, [A], h_A, [], a, X, TTL)$

$A \rightarrow *:$ (P_A)

B :

$h_B = H(B, h_A), P_B = (QRREQ, S, D, [A, B], h_B, a, X, TTL)$

$B \rightarrow *$: (P_B)

Step3: Destination node D recomputed h'_B (i.e. $h'_B = H(B, (H(A, (P_s))))$ from P_B. If $h'_B = h_B$, it verifies that no node modification has been done during en-route phase.

4. UNIPATH DISCOVERY OPERATIONS PERFORMED BY DESTINATION NODE

Since the network is multi-hop in nature, the free slots recorded at each node may be different. The set of common free slots between two adjacent nodes denotes the link bandwidth between them. So in the hop-by-hop approach, we firstly find the link bandwidth of all links in given path. Consider a path $\{S, A, B, D\}$ from source S to destination D, Let a, b, c denotes the free time slot of links (S, A), (S, B) and (S, D) respectively. For this path, a slot reservation follows the order of $\vec{SA}$, $\vec{AB}$, and $\vec{BD}$. In this a maximal reserved time-slot number is used to denote the largest number of time slots of a link in a path. If $a = [2,5,9,10], b = [1,5,8,9]$ and $c = [1,6,8,9]$, then $< 2,5,10 >$ is reserved in to the link $\vec{SA}$, $< 1,8,9 >$ is reserved in $\vec{AB}$ and $< 6 >$ is in to link $\vec{BD}$ as shown in Figure 2. The minimum reserved time-slot number of $\vec{SA}$, $\vec{AB}$, and $\vec{BD}$ is 1. So, bandwidth of path $\{S, A, B, D\}$ is 1 using hop-by-hop reservation.

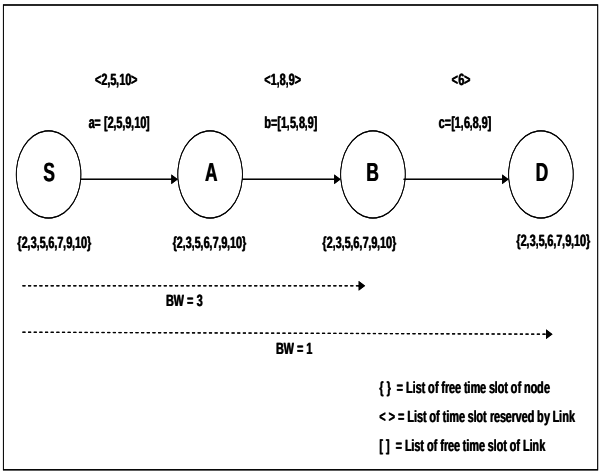

Fig 2: Bandwidth Reservation by Hop-by-Hop Approach

In order to increase the path bandwidth as made available during hop-by-hop reservation, extra efforts are required. To achieve this, we proposed a unipath discovery operation/path bandwidth calculation algorithm that does not follow the traditional hop-by-hop approach to determine the end-to-end path bandwidth X. The unipath discovery operation determines its maximum path bandwidth by constructing a least-cost-first reservation tree T_{LCF}. Before constructing T_{LCF}, a time-slot reservation tree T is constructed using breadth-first-search approach in the following manner:

Given a path $\{S, A, B, D\}$, let the root of T be represented as abc, where *a* represents the bandwidth i.e. set of free-slots of link (S, A) and b represents the bandwidth of link (A, B).Let $\underline{ab}$ denote the time-slots that are reserved on links *a* and *b*. Child nodes of root are $\underline{ab}c$ and $a\underline{bc}$ which form the first level of tree T. The tree T recursively expands all child nodes of each node on each level of tree T, and follow the same rules as that of the first level of tree T until the leaf nodes are reached. Each path from root to leaf nodes gives a time-slot reservation pattern. To reduce the time needed to search a path satisfying a given bandwidth requirement X, a least-cost-first time–slot reservation tree T_{LCF} is constructed from the time-slot reservation tree T as follow:

The child nodes on each level of tree T are sorted in ascending order from left to right by using the number of reserved time-slots on them. All T and T_{LCF} trees diagram of the Figure 1. Are shown below in Figure 3(a-f). The comparison of end to end bandwidth using hop by hop and least cost first reservation approach is shown in Figure 4.

.

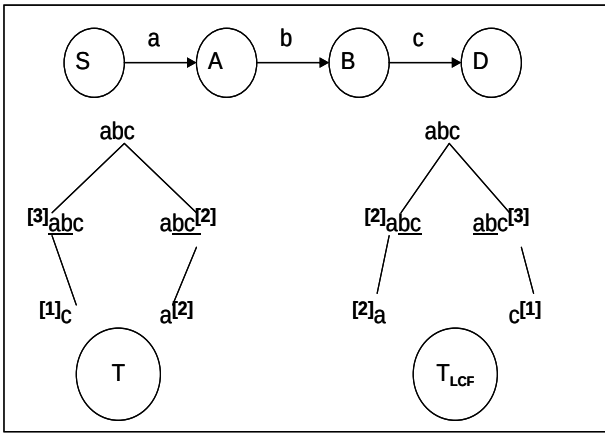

Fig 3: (a) Time Slot (T) and Least Cost First (T_{LCF})Reservation tree of path (S, A, B, D)

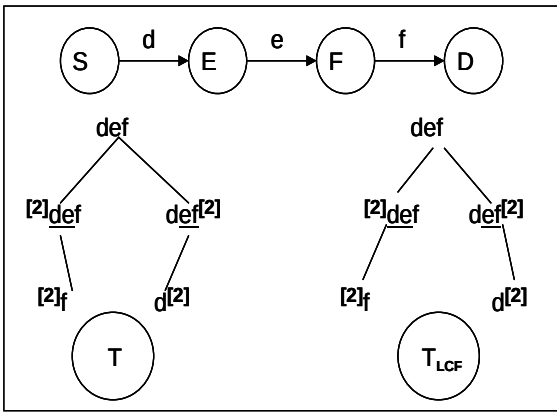

Fig 3: (b) Time Slot (T) and Least Cost First (T_{LCF}) Reservation tree of path (S, E, F, D)

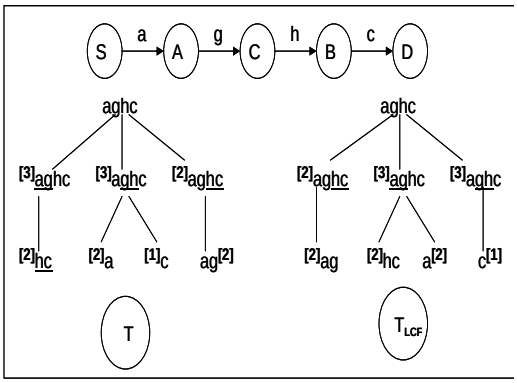

Fig 3: (C) Time Slot (T) and Least Cost First (T_{LCF}) Reservation tree of path (S, A, C, B, D)

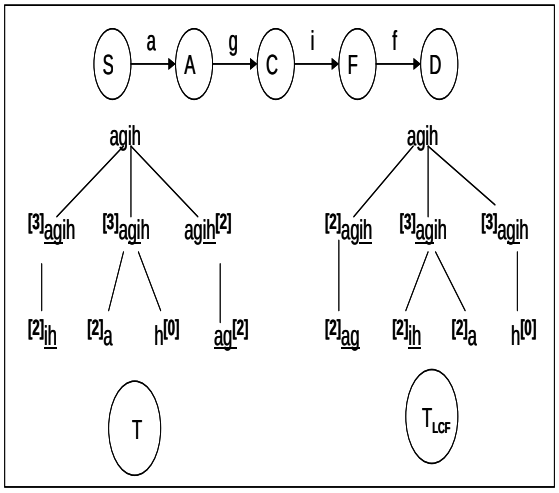

Fig 3: (d) Time Slot (T) and Least Cost First (T_{LCF}) Reservation tree of path (S, A, C, F, D)

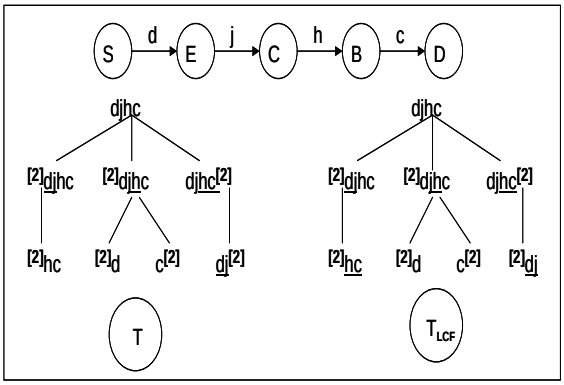

Fig 3: (e) Time Slot (T) and Least Cost First (T_{LCF}) Reservation tree of path (S, E, C, B, D)

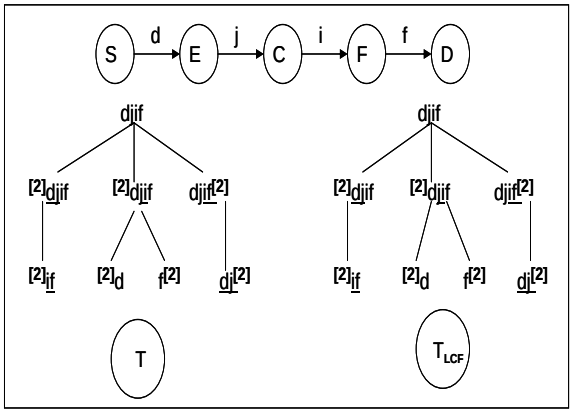

Fig 3: (f) Time Slot (T) and Least Cost First (T_{LCF}) Reservation tree of path (S, E, C, F, D)

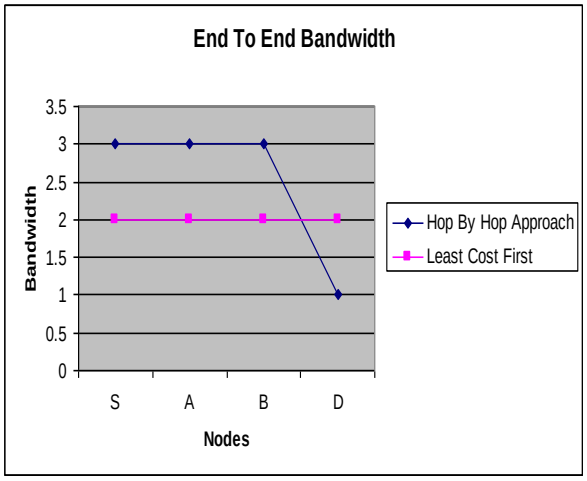

Fig 4: End to End Bandwidth by Hop-by-Hop and Least Cost First Reservation Approach of path (S, A, B, D)

5. MULTIPATH DISCOVERY OPERATION PERFORMED BY DESTINATION

The multipath discovery operation is to sequentially exploit multiple unipaths such that the total sum of path bandwidths fulfills the original path bandwidth X . A centralized algorithm is proposed at destination to determine the multipath. Given the required path bandwidth is $X,$ the multi-path discovery algorithm is formally described as below:

Step1: Let $\text{Bandwidth}\_\text{sum}$ denote the total sum of bandwidth of multiple unipaths. Initially, $\text{Bandwidth}\_\text{sum} = 0;$

Step2: A unipath discovery procedure is applied at destination to search all T_{LCF} trees using depth-first search technique and to find a new QoS path from source to destination having a maximal path bandwidth. If there exists more than one path satisfying the maximum bandwidth b, then chooses a path having minimum hop count. Let $\text{Bandwidth}\_\text{sum} = \text{Bandwidth}\_\text{sum} + b$, apply the same unipath discovery procedure until $\text{Bandwidth}\_\text{sum} \geq X$. If for the same network the bandwidth requirement between source S and destination D is 4, then the QoS enabled paths shown in Figure 5 are chosen by destination using multipath discovery algorithm.

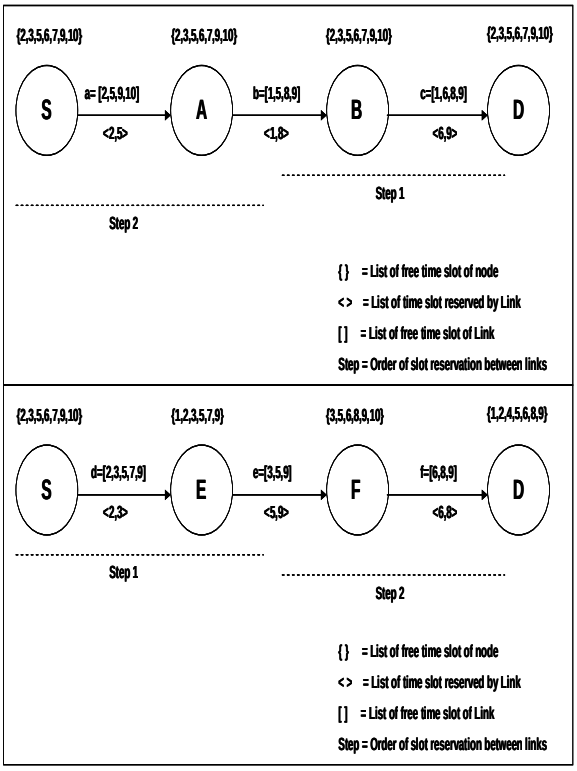

Fig 5: Unipath Found by Multipath Discovery Algorithm

6. SECURE UNICASTING OF QRREP PACKETS TO SOURCE NODE

Step1: Destination node D generates a reply packet which contains the following fields (destination id, source id, node history, bandwidth requirement and TTL field) i.e. $P_D = \{(QRREP, D, S, [S, A, B, ku_B[D]], X, TTL)\}$, encrypted reservation pattern of chosen path and $M_D = HMAC_{K_{SD}}(P_D)$ (which contain MAC code of P_D with symmetric key K_{SD}). After determining a multipath, node D initiates a secure QRREP packet unicast to source node S. The following sequence is adopted by destination D to unicast secure QRREP packet on path (D, B, A, S):

$$D \rightarrow B$$
$$P_D = \{(QRREP, D, S, [S, A, B, ku_B[D]], X, TTL)\}$$
$$B \rightarrow A$$
$$P_D = \{(QRREP, D, S, [S, A, ku_A[B, ku_B[D]], X, TT$$
$$A \rightarrow S$$
$$P_D = \{(QRREP, D, S, [S, Ku_S[A, ku_A[B, ku_B[D]]], X, TTL)\}$$

Step 2: Every intermediate node receives the packet encrypt its ID with previous node public key. So that the node only the next node ID.

$$B \rightarrow A$$
$$P_D = \{(QRREP, D, S, [S, A, ku_A[B, ku_B[D]], X, TTL)\}$$

Step 3: Similarly Node A encrypt their ID with public key of S (ku_S). So that node S know only next node is A rest of the path is not known so that there will be no denial of service/modification attack feasible

$$A \rightarrow S$$
$$P_D = \{(QRREP, D, S, [S, Ku_S[A, ku_A[B, ku_B[D]]], X, TTL)\}$$

7. CONCLUSION

The goal of the proposed protocol is to explore efficient multipath routing and QoS provisioning in term of bandwidth and security. So in terms of bandwidth, it has better call acceptance rate in ad hoc networks where finding a single path satisfying all QoS requirements is very difficult. Another benefit of proposed protocol is that, it can provide fault tolerance, load balancing and reduce the route discovery delay. The proposed protocol also offers detection of several malicious behaviors and robustness under most of routing attacks (e.g. spoofing, node deletion, node insertion, modification, fabrication, routing loops and denial of service attacks), while minimizing the cryptographic computational overhead.

8. REFERENCES

[1] C. Siva Ram Murthy and B. S. Manoj, AdHoc Wireless Networks: Architectures and Protocols. Prentice Hall, 2004.

[2] S. H. Shah and K. Nahrstedt, " Distributed Quality-of-Service Routing in Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1488-1504, August 1999.

[3] M. K. Marina and S. R. Das, "Ad hoc On-demand Multipath Distance Vector Routing," Technical Report, Computer Science Department, Stony Brook University, April 2003.

[4] S. J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," Proceeding of IEEE International Conference on Communications (ICC 2001), pp. 3201-3205, Helsinki, 2001.

[5] S. De, S.K. Das, H. Wu, and C. Qiao," Trigger –Based Distributed QoS Routing in Mobile Ad Hoc Networks," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6(3), pp. 22-35, July 2002.

[6] L. Chen and W. Heinzelman, " QoS-aware Routing Based on Bandwidth Estimation for Mobile Ad Hoc Networks," IEEE JSAC, Special Issue on Wire-less Ad Hoc Networks, vol. 23(3): pp. 561–72, March 2005.

[7] Y. Hwang and P. Varshney, "An Adaptive QoS Routing Protocol with Dispersity for Ad hoc Networks," Proceeding of the 36th Hawaii International Conference on System Sciences (HICSS'03), January 2003.

[8] P. Sinha, R. Sivakumar, and V.Bharghavan, "CEDAR: A Core-Extraction Distributed Ad hoc Routing Algorithm," Proceeding of 18th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '99), New York, NY, pp. 202-209,March 1999.

[9] C.R. Lin, "On-demand QoS Routing in Multi-Hop Mobile Networks," Proceeding of IEEE INFOCOM 2001, The Conference on Computer Communications, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1735- 1744, April 2001.

[10] Xuefei Li, "Multipath Routing and QoS Provisioning in Mobile Ad hoc Networks" In PhD. Thesis, Department of Electronics Engineering, Queen Mary, University of London, pp. 1-153, April 2006.

[11] Saida Ziane,Abdelhamid Mellouk, "A Swarm Intelligent Multi-path Routing for Multimedia Traffic over Mobile Ad hoc Networks" Proceeding of (Q2SWinet'05),Montreal, Quebec, Canada, pp.55-62,October 2005.

[12] Supachote Lertvorratham "Integrated Secure Multipath Mobile Ad Hoc Network" PhD thesis, pp.1-113, 2010.