Secure Framework for Voice Transmission over Multipath Wireless Ad-hoc Network

Binod Vaidya
Instituto de Telecomunicações,
Covilhã, Portugal
email: bnvaidya@co.it.pt

Mieso K. Denko
Dept. of Computing & Information Science,
University of Guelph,
Guelph, Canada
email: denko@cis.uoguelph.ca

Joel J. P. C. Rodrigues
Instituto de Telecomunicações,
University of Beira Interior,
Covilhã, Portugal
email: joeljr@ieee.org

***Abstract*—With the growth of the Internet services, Voice over IP (VoIP) has been playing a key role in cutting the costs of telephone calls. It can be seen that since the demand of VoIP over wireless network is growing, the use of VoIP over Mobile Ad-hoc Network (MANET) is expected to grow as well. We have identified some of the challenging issues to ensure robust and secure voice communication over MANET. In this paper, we depict a framework for secure voice transmission over multipath wireless mobile ad-hoc network. We also propose an efficient traffic allocation approach for multipath wireless mobile ad-hoc network in order to deliver real-time traffic over it. We conduct series of simulations to evaluate such a framework through different performance metrics.**

***Index Terms*—wireless ad-hoc network; multipath routing; voice transmission; security.**

I. Introduction

Mobile ad-hoc networks (MANETs), being self-organized wireless multihop networks, allow mobile nodes to internetwork without any preexisting infrastructure. On-demand routing protocol such as Ad hoc On-demand Distance Vector (AODV) [1] is well-suited in dynamic ad-hoc networks because they maintain only the actively used routes. However, in a single-path routing, previously created multihop route could frequently break because of node mobility. New route discovery would initiate for each failure, in turn, inducing routing overheads and latency. A multipath routing protocol is a promising technique to overcome problems of frequent topological changes and link instability as the use of multiple paths could diminish effect of possible node and link failures. Thus multipath ad-hoc routing protocols are deemed superior over single-path routing protocols as the former provide robustness, increase reliability, reduce end-to-end delay, provide load-balancing, and improve security [2].

With the increasing growth of the Internet uses, Voice-over-IP (VoIP) has emerged as a viable way to drastically cut costs of telephone calls. As the demand of VoIP over wireless network is growing, the use of VoIP over MANET is expected to grow as well.

It is still quite challenging to ensure robust and secure voice communication in MANET. This paper presents a secure framework for voice transmission over wireless mobile ad-hoc network that not only is robust against frequent communication failure and adverse environment but also provides efficient traffic allocation approach for real-time traffic delivery.

The rest of this paper is organized as follows: Section II presents related work, while Section III describes issues on voice transmission over MANET. Section IV shortly illustrates our previous work related to the proposed work, and Section V describes a proposed framework for secure voice transmission over multipath MANET. Section VI gives security analysis of proposed scheme, whereas Section VII provides performance evaluation. And finally Section VIII concludes the paper and points out future research directions.

II. Related Work

In this section, we review some of related works to our framework. Some of well-known multipath protocols based AODV are Ad hoc On-demand Multipath Distance Vector (AOMDV) [3], and Ad hoc On-Demand Distance Vector Multipath (AODVM) [4].

The authors in [5] introduced multistream coding with multipath transport (MPT) for video traffic over ad hoc network. In their approach, a video bit stream is divided into several substreams and then packets from different substreams are sent over different paths.

However, none of above-mentioned schemes have considered any security mechanisms.

Some of security schemes for wireless ad-hoc routing protocols are Secure Multipath Routing (SecMR) [6] and Secure, Disjoint, Multipath Source Routing (SDMSR) [7] which are designed for multipath routing security. Several protocols such Papadimitratos and Haas [8] and Lou *et al.* [9] using multiple paths between source and destination to provide secure data transmission in wireless ad hoc networks have been studied.

Gibson *et al.* [10] have combined a selective encryption scheme with scalable MPEG-4 coding technique and showed that encryption of the core layer only is sufficient to ensure a high level of protection against eavesdroppers, thus significantly reducing the signal processing power needed for encryption and decryption in comparison to encryption of the full bitstream. Lindskog *et al.* [11] have proposed a content-independent model for scalable encryption that is based on a selective encryption paradigm.

978-1-4244-4148-8/09/$25.00 ©2009

In this paper, we propose a secure framework for voice transmission over multipath MANET using an efficient traffic allocation approach and selective encryption paradigm.

III. Voice Transmission over MANET

Voice over IP (VoIP) is a technology for transmitting voice, such as telephone calls, over packet-switched data networks. Real-time transport protocol (RTP) on the top of User Datagram Protocol (UDP) is used as protocol for transporting voice packets to the destination (callee). Whereas signaling protocol such H.323 and Session Initiation Protocol (SIP) is used to to create and manage real-time connections in VoIP systems.

The most popular ITU-T codec used in VoIP applications are G.711, G.723.1, G.726, and G.729 [12].

Scalable audio coding [13] is widely used for multimedia streaming but not significantly used for VoIP application. It consists of a core bitstream that provides acceptable voice quality, and when enhancement bitstreams combined with a core bitstream, provide improved voice quality. The ITU-T standard for scalable audio coding is G.727, which is based upon adaptive differential PCM (ADPCM) and operates at data rates of 16kbps to 40kbps. The core bitrate is 16kbps, and up to three 8kbps enhancement layers can be included.

In order to improve reliability of transmission over MANET is to use path diversity as the probability of all the paths breaking down simultaneously is low, the probability of packet loss is reduced. Further, to address QoS requirements in MANETs, scalable audio coding technique can be used as it is promising technique for robust real-time multimedia communication over lossy networks.

As vulnerabilities may affect the route discovery process of multipath routing protocols, allowing malicious nodes to control the routing paths, both the multipath routing process and data transfer phase should be well protected.

IV. AODV-MAP Scheme

In the paper [14], we proposed a robust multipath routing scheme, AODV with Multiple Alternative Paths (AODV-MAP) for wireless ad-hoc network, which is a modification of AODV protocol [1]. This scheme is intended for ad-hoc networks in which communication failures occur frequently and designed to compute node-disjoint paths as well as fail-safe paths [15]. So the combination of node-disjoint and fail-safe paths allows the computation of more multiple paths than in node-disjoint or link-disjoint routing alone. The features of the proposed scheme are path accumulation, selective route request (RREQ) forwarding scheme, multiple alternative path discovery, and path label setting. And its main goal is to lower frequencies of costly route discoveries so it can keep end-to-end connection for longer time.

For instance, as shown in Fig. 1, number of multiple paths between source *S* and destination *D* can be discovered during route discovery process.

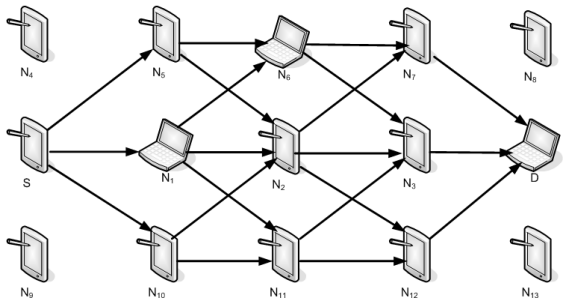

Fig. 1. Discovering multiple paths during route discovery.

A. Secure AODV-MAP

It is desired that the multipath routing protocol should be robust not only against dynamically changing topology but also against malicious attacks. In the paper [16], we proposed secure AODV-MAP (SAODV-MAP) scheme since AODV-MAP scheme is vulnerable to various attacks.

In order to achieve secure routing in fully distributed environment, we considered threshold cryptography scheme and self-certified public keying.

However, it should be noted that the security scheme is needed not only for ad-hoc routing but also for data delivery.

V. Secure Framework for Voice Transmission over multipath MANET

We depict a framework for robust and secure voice transmission over multipath MANET. For this purpose, we use robust multipath routing scheme (AODV-MAP) for wireless mobile ad-hoc network along with an efficient traffic distribution approach.

A. Traffic allocation approach using AODV-MAP scheme

We propose a traffic allocation approach by using AODV-MAP scheme and scalable audio coding technique for voice transmision in multipath multihop wireless network. In this approach, we consider G.727 (ADPCM) with a core layer and one enhancement layer.

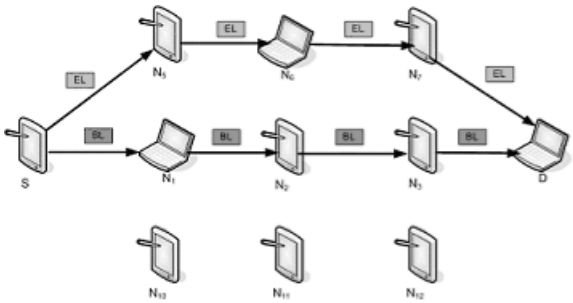

Fig. 2. Initial traffic distribution in AODV-MAP.

At the initial, the source node begins to send core bitstream or base layer (BL) on the primary path and enhancement bitstream or layer (EL) on the node-disjoint path. Since the primary path and the node-disjoint path are not correlated,

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

TABLE I
NOTATIONS USED IN PROPOSED SECURITY SCHEME

$\langle M \rangle K$	MAC value of message M under key K
IP_S, IP_D	IP address of source and destination
SN_S, SN_D	Sequence numbers of source and destination
$RREQ\_ID$	A sequence number
hop_cnt	The value of hop count
$route\_path$	Path accumulation list of the route path
CM_S	Cumulative MAC computed by source S with shared key between *S* and *D* over $AUTH$
CM_i	Cumulative MAC computed by node N_i with shared key between itself and *D* over the the cumulative MAC in the received RREQ
$path\_label$	type of path to determine primary, node-disjoint or fail-safe paths
SK_S, SK_D	session key generated by *S* and *D* respectively
SK_{SD}	joint session key of SK_S and SK_D
$\{M\}K$	Encryption of message M with key K

source node uses the node-disjoint path to provide load balancing. Generally, a multihop path is up or down for random periods of time, leading to bursty packet losses. According the proposed approach, when forwarding paths break, base layer or enhancement layer can be forwarded through different paths in the routing table.

For instance, initially BL is forwarded through the primary path ($S-N_1-N_2-N_3-D$) whereas EL is forwarded through the node-disjoint path ($S-N_5-N_6-N_7-D$) as shown in Fig. 2.

The further traffic distribution is as follows:

- In case of BL forwarding, if the primary path breaks, the proposed approach first finds fail-safe path for each node on the primary path as it has higher packet delivery rate. So it uses one of fail-safe paths to forward BL to the intended destination. If no fail-safe paths are available then only it uses node-disjoint path to forward BL to the intended destination.
- In case of EL forwarding, the proposed approach first finds fail-safe path. If no fail-safe paths are available then only it uses primary path.

B. Proposed security mechanism

The proposed security scheme provides complete solution for both ad-hoc routing and for data delivery, a modified SAODV-MAP is obtained. Table I shows the notation used in proposed security scheme.

1) Modified Secure Route Discovery: The modified route discovery phase involves not only the establishment of secure multiple alternative paths between the source and destination nodes but also session key distribution.

A source *S* initiates route discovery for a destination node *D* as per AODV-MAP scheme. The source *S* generates a session key (SK_S)and XORed with the shared key (K_{SD}) to get the following:

$SK_{SE} = SK_S \oplus K_{SD}$.

The source computes and appends HMAC to RREQ that covers non-mutable fields $RREQ\_ID, IP_S, IP_D$, (SN_S, SN_D), and SK_{SE}.

The source *S* computes $AUTH$ with the shared key (K_{SD}) and CM_S over $AUTH$ along with other mutable fields such as $hop\_cnt, route\_path$.

The source *S* will broadcast RREQ to its neighbors. A RREQ message received by an intermediate node is processed as specified in AODV-MAP scheme.

The intermediate nodes can forward duplicate RREQ as per the selective RREQ forwarding scheme as specified in AODV-MAP scheme.

The route request process is as follows:

$$
\begin{aligned}
S &: AUTH = \langle IP_S, IP_D, SN_S, SN_D, BcstID, \\
&\quad SK_{SE} \rangle K_{SD} \\
&: CM_S = \langle AUTH, hop\_cnt, route\_path \rangle K_{SD} \\
S \Rightarrow * &: (RREQ, IP_S, IP_D, SN_S, SN_D, BcstID \\
&\quad hop\_cnt, route\_path, AUTH, CM_S) \\
B &: CM_B = \langle CM_S, hop\_cnt, route\_path \rangle K_{BD} \\
B \Rightarrow * &: (RREQ, IP_S, IP_D, SN_S, SN_D, BcstID \\
&\quad hop\_cnt, route\_path, AUTH, CM_B) \\
C &: CM_C = \langle CM_B, hop\_cnt, route\_path \rangle K_{CD} \\
C \Rightarrow * &: (RREQ, IP_S, IP_D, SN_S, SN_D, BcstID \\
&\quad hop\_cnt, route\_path, AUTH, CM_C)
\end{aligned}
$$

When the RREQ packet arrives at the destination *D*, it verfies keyed-MAC from the source as well as cumulative MAC from nodes that participated in RREQ forwarding and illegitimate requests are discarded. The destination also checks SN_D in incoming RREQ packets and discards stale requests. It also XORed SK_{SE} with K_{SD} to obtain SK_S as follows:

$SK_S = SK_{SE} \oplus K_{SD}$.

SK_S will be used for secure real-time data exchange.

If the verification is successful, the destination *D* can be assured that this RREQ was really originated from the source *S*, and every node listed in $route\_path$ participated in the RREQ forwarding.

It should be noted that in SAODV-MAP scheme, destination *D* is responsible for discovering primary path, node-disjoint paths and fail-safe paths as specified in AODV-MAP scheme.

After successful verification, the destination *D* generates a session key (SK_D). The destination also encrypts the session key with the shared key (K_{SD}) by XOR operation, which is as follows:

$SK_{DE} = SK_D \oplus K_{SD}$.

Then destination *D* generates a route reply (RREP) message. The RREP message contains $AUTH_1$ having the identifiers of the source and destination nodes, the accumulated route as obtained from the RREQ message, and other information along with a HMAC.

The RREP packet is then sent back on the reverse route as given by the accumulated route ($route\_path$) till the RREP reaches the source node *S*. The route reply process is as

978-1-4244-4148-8/09/$25.00 ©2009

follows:

$$
\begin{aligned}
D &: AUTH_1 = \langle IP_S, IP_D, SN_D, route\_path, \\
&\quad path\_type, SK_{DE} \rangle K_{DS} \\
&: HMAC_{K_{DC}} = \langle AUTH_1, hop\_cnt \rangle K_{DC} \\
D \Rightarrow C &: (RREP, IP_S, IP_D, SN_D, route\_path, \\
&\quad path\_type, hop\_cnt, AUTH_1, HMAC_{K_{DC}}) \\
C &: HMAC_{K_{CB}} = \langle AUTH_1, hop\_cnt \rangle K_{CB} \\
C \Rightarrow B &: (RREP, IP_S, IP_D, SN_D, route\_path, \\
&\quad path\_type, hop\_cnt, AUTH_1, HMAC_{K_{CB}}) \\
C &: HMAC_{K_{BS}} = \langle AUTH_1, hop\_cnt \rangle K_{BS} \\
B \Rightarrow S &: (RREP, IP_S, IP_D, SN_D, route\_path, \\
&\quad path\_type, hop\_cnt, AUTH_1, HMAC_{K_{BS}})
\end{aligned}
$$

Once source *S* receives RREP message, it verifies whether it received the message from its neighbor and if this neighbor is the first node on the path. If so, it verifies the signatures of all the nodes in the reply. The path is then accepted to be valid if all the signatures are verified. The source *S* decrypts the session key generated by the destination (SK_D) as well. The obtained session key (SK_D) will be used for secure real-time data exchange.

2) Secure Real-time traffic transmission: During this phase, a content-dependent scalable encryption approach is used that aims to provide different protection levels according to different layers. The basic idea in this approach is to apply encryption to base or core layer using joint session key (SK_{SD}), whereas the enhancement layers are encrypted by bitwise XOR operation with joint session key (SK_{SD}).

At the source *S*, SK_{SD} is computed. If it is base layer, it is encrypted with SK_{SD} and then it sends the encrypted data along with HMAC to the destination. If it is enhancement layer, it is encrypted using bitwise XOR operation and then it sends the encrypted data along hash function to the destination. The algorithm for sending substream is as follows.

1. Compute $SK_{SD} = SK_S \oplus SK_D$
2. If *substream is base layer* then
3. Compute $E_{SK_{SD}}(BL) = \{DATA\}_{SK_{SD}}$
4. Compute $HMAC_{SK_{SD}} = \langle E_{SK_{SD}}(BL) \rangle K_{SD}$
5. Send $E_{SK_{SD}}(BL), HMAC_{SK_{SD}}$
6. else compute $E_{SK_{SD}}(EL) = \{DATA\} \oplus SK_{SD}$
8. Compute $H'_{EL} = H(E_{SK_{SD}}(EL))$
9. Send $E_{SK_{SD}}(EL), H_{EL}$

At the destination *D*, SK_{SD} is computed first. If it is base layer, D will compute $HMAC'_{SK_{SD}}$ and compare it with the received $HMAC_{SK_{SD}}$ for verification. Then *D* decrypts with SK_{SD}. If it is enhancement layer, D will compute H'_{EL} and compare it with the received H_{EL} for verification. And it is decrypts using bitwise XOR operation. The algorithm for receiving substream is as follows.

1. Compute $SK_{SD} = SK_S \oplus SK_D$
2. If *incoming substream is base layer* then
3. Compute $HMAC'_{SK_{SD}} = \langle E_{SK_{SD}}(BL) \rangle K_{SD}$
4. If $HMAC'_{SK_{SD}} = HMAC_{SK_{SD}}$ then
5. Decrypt $E_{SK_{SD}}(BL)$ with SK_{SD}
6. else discard
7. else compute $H'_{EL} = H(E_{SK_{SD}}(EL))$
8. If $H'_{EL} = H_{EL}$ then
9. Decrypt $E_{SK_{SD}}(BL)$ by XORing with SK_{SD}
10. else discard

VI. Security Analysis

We analyze the security of such a framework by evaluating its robustness in the presence of some of the attacks. Mainly attacks targeting wireless ad-hoc networks are eavesdropping, modification, fabrication, replay, impersonation, dropping of packets and denial of service.

1) Protection from modification:
In the modified SAODV-MAP scheme, non-mutable fields are protected by AUTH. So no node can impersonate the source *S* to fabricate RREQ due to the lack of K_{SD} known only to *S* and *D*. Any modification on such fields can be easily detected by destination *D*. Furthermore, in modified SAODV-MAP scheme, the authenticity of these mutable fields is guaranteed by integrating them into the computation of CM_i. During data delivery, real-time traffic is encrypted.

2) Protection from impersonation:
The modified SAODV-MAP prevents IP or MAC spoofing by storing public keys along with neigbhors' identities in neighbor-node table during the neighbor discovery phase, During route discovery, since HMAC shared key is used, not only to verify authenticity of the communicating nodes but also the intermediate nodes that participated in RREQ forwarding thus nodes cannot spoof other nodes in route instantiation. The use of threshold cryptography makes the impersonation attacks more difficult. While during data delivery, HMAC with session key is used for base layer and hash function is used for enhancement layer.

3) Protection from fabrication:
This scheme does not use the routing information present within intermediate node caches, but accepts RREP messages only from the destination node so cache poisoning cannot take place. The modified SAODV-MAP defeats the RERR fabrication attack because all RERR messages are marked by keyed-MAC that ensures authenticity and integrity of RERR messages. While during data delivery, HMAC with session key is used for base layer and hash function is used for enhancement layer. That ensures authenticity and integrity of voice traffic.

4) Protection against packet dropping:
An adversary either selectively or completely drops packets and so succeeds in disrupting the normal operation of the network.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

The modified SAODV-MAP scheme can thwart black hole attacks by finding multiple alternative paths between source and destination pair and by disabling the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node.
In this scheme as scalable coding being used, if enhancement layers are dropped, the voice traffic can be received with little degrade in quality. Only if the base layer is dropped then other bit streams will be useless.

5) Data confidentiality:
In case of real-time traffic delivery, a scalable encryption is used so that the base layer is encrypted with session key SK_{SD}. As joint session key SK_{SD} is known to only sender and receiver, data confidentaility can be provided. Whereas the enhancement layer use only encryption using bitwise XOR operation, which is fast and lightweight algorithm.

VII. Performance Evaluations

To evaluate the performance of the proposed framework for robust and secure voice transmission over multipath MANET, we have conducted series of simulations using OPNET Modeler [17].

An experiment has been conducted under benign condition.

In simulations, MANET consists of sixteen mobile nodes which are located inside a 600m x 600m region. Each node is randomly placed in the region initially. We consider a popular random waypoint mobility model. We have used a pause time of 1.0s for all the experiments. The speed of the nodes varies from 0m/s to 10m/s. We use the IEEE 802.11 protocol in the MAC layer working in the DCF mode. The channel has a bandwidth of 1Mb/s. The transmission range is 250 m. UDP is used as transport protocol. For the traffic model of the VoIP session, G.727 codec is considered. Simulation duration is set for 300 seconds.

For ad hoc network using proposed scheme, we evaluated following three performance metrics: packet delivery ratio, average end-to-end delay and normalized routing load.

We have considered three scenerios for our experiment under benign environment: i) first scenerio is a framework with G.727 codec using AODV scheme; ii) second scenerio is a framework with G.727 codec using AODV-MAP scheme; iii) three scenerio is a framework with G.727 codec using modified SAODV-MAP.

Under benign environment, the AODV, AODV-MAP and the modified SAODV-MAP are compared in order to verify the cost of the proposed scheme.

A. Simulation Results

In order to analyze the simulation results for the framework for voice communication in multipath MANET, we compare performance of the modified SAODV-MAP with AODV-MAP and AODV in terms of packet delivery rate, average end-to-end delay and normalized routing load with respect to max speed.

Figure 3 shows the packet delivery ratio plotted against maximum speed for AODV, AODV-MAP and modified SAODV-MAP. As the velocity of nodes increases, the probability of link failure increases and hence the number of packet drops also increases. It can be seen that the packet delivery rate in the AODV scheme is lower than other two schemes. Whereas AODV-MAP scheme and modified SAODV-MAP scheme produce high packet delivery ratio due to presence of multiple paths. So when an active routing path is broken due to mobility of nodes, these protocols still can manage the communication between source and destination without interrupt. As shown in Fig. 3, the packet delivery ratio obtained using modified SAODV-MAP is above 90% for almost all the node speed and is very close to that of AODV-MAP. This suggests that modified SAODV-MAP is effective in discovering and maintaining routes for delivery of data packets, even with high node mobility. In order to ensure the quality of VoIP session, average packet delivery rate should be high.

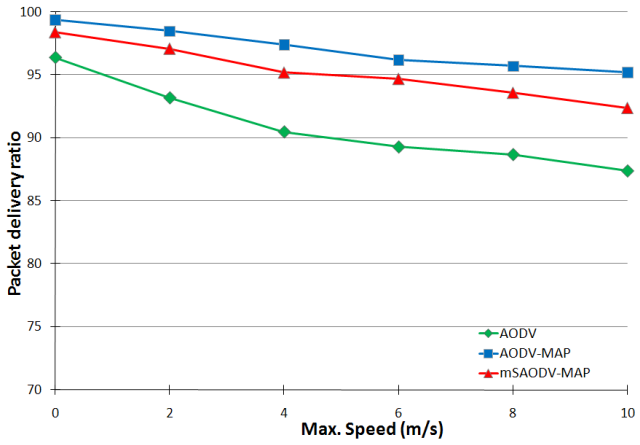

Fig. 3. Packet delivery ratio

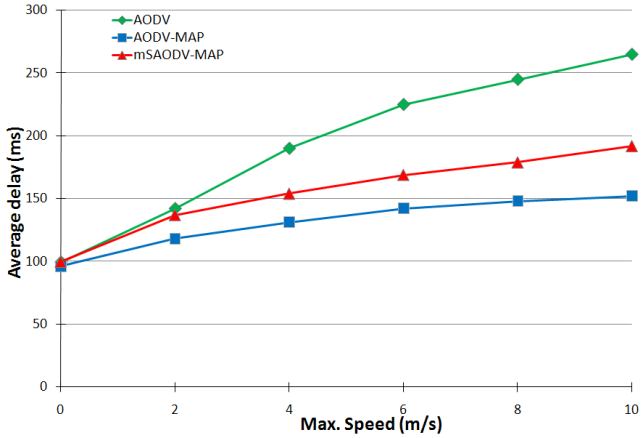

Fig. 4. Average end-to-end delay

Figure 4 illustrates the change in the average end-to-end delay as a function of speed of nodes for AODV, AODV-MAP and modified SAODV-MAP schemes. For all the scenarios, it can be seen that there is increase in average delay

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

with the increase of node speed. AODV-MAP and modified SAODV-MAP schemes provide smaller packet delay than AODV scheme. Delays of AODV-MAP scheme and modified SAODV-MAP are gradually increased after node velocity of 4m/s, while delay in AODV increases quickly as velocity increases. This is because availability of alternate paths in AODV-MAP and modified SAODV-MAP eliminate route discovery latency that contributes to delay when active route fails. However, modified SAODV-MAP scheme has end-to-end delay slightly higher than that of AODV-MAP because of cryptographic operations during route discovery and data delivery.

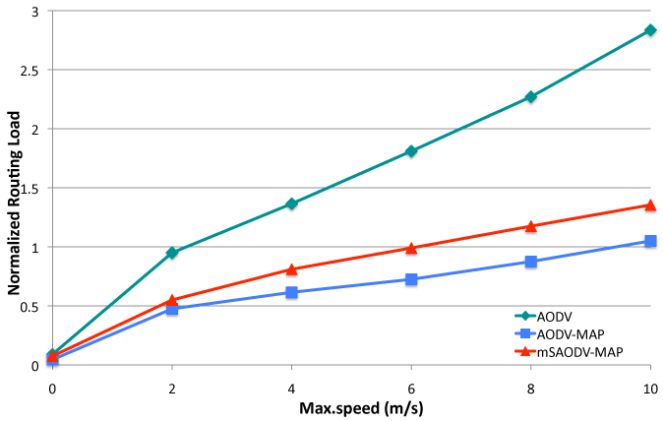

Fig. 5. Normalized Routing Load.

Figure 5 presents the normalized routing load characteristics for AODV, AODV-MAP and modified SAODV-MAP schemes. It can be seen that the normalized routing load in AODV-MAP and modified SAODV-MAP schemes perform much better than that of AODV. The normalized routing load in AODV increases more quickly than those in AODV-MAP and modified SAODV-MAP schemes with the increase of node speed. For AODV-MAP and modified SAODV-MAP schemes, it increases slowly with the increase of node speed. Since AODV-MAP and modified SAODV-MAP schemes can find multiple alternate route paths in a route discovery process, the protocols tremendously decrease the number of route rediscovery process. Whereas, since AODV encounters more link failures with the increase in mobility, it has to trigger more new route discovery process which causes more routing control packets to be sent to the whole networks.

VIII. Conclusion and Future Work

In this paper, a robust and secure framework for voice transmission over multipath MANET has been proposed. Proposed framework is robust not only against dynamically changing topology but also against adverse environment. We have provided security analysis of the proposed scheme as well as performance evaluation of above framework. Simulations showed that the performance of the proposed scheme is much better than AODV routing in terms of various performance metrics. The simulation results show that modified SAODV-MAP scheme is as efficient as AODV-MAP scheme.

The limitation of this scheme is that it cannot withstand dropping of substream data containing base layer. In order to improve it, we can apply unequal error protection (UEP) to the base layer.

In future works, we will conduct more experiments to verify robustness of the proposed framework under adverse environments. Furthermore, we will provide a formal analysis of the proposed secure framework for multipath wireless adhoc network.

Acknowledgment

Part of this work has been supported by *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Portugal.

References

[1] C.E. Perkins, E. Belding-Royer, and S. R. Das, "Ad hoc on-demand distance vector (AODV) routing", *IETF RFC 3561*, Jul 2003.
[2] S. Mueller, R. P. Tsang, and D. Ghosal, "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges", *Performance Tools and Applications to Networked Systems*, LNCS 2965, 2004, pp. 209–234.
[3] M. K. Marina, and S. R. Das, "Ad hoc on-demand multipath distance vector routing", *Wiley Wireless Communications and Mobile Computing*, vol. 6, no. 7, 2006, pp. 969–988.
[4] Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A routing framework for providing robustness to node failures in mobile ad hoc networks", *Elsevier Ad Hoc Networks Journal*, vol. 2, no. 1, 2004, pp. 87–107.
[5] S. Mao, S. Lin, Y. Wang, S. S. Panwar, and Y. Li, "Multipath video transport over ad hoc networks", *IEEE Wireless Communications*, vol. 12, no. 4, Aug. 2005, pp. 42–49.
[6] R. Mavropodi, P. Kotzanikolaoua, and C. Douligerisa, "SecMR–a secure multipath routing protocol for ad hoc networks", *Elsevier Ad Hoc Networks Journal*, vol. 5, 2007, pp. 87–99.
[7] S Berton, H. Yin, C. Lin, and G. Min, "Secure, Disjoint, Multipath Source Routing Protocol (SDMSR) for Mobile Ad-Hoc Networks, In *Proc. of GCC'06*, 2006, pp. 387–394.
[8] P. Papadimitratos, and Z. J. Haas, "Secure Data Communication in Mobile Ad hoc Networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, 2006, pp. 343–356.
[9] W. Lou, W. Liu, Y. Zhang, and Y. Fan, "SPREAD: Improving network security by multipath routing in mobile ad hoc networks", *Springer Wireless Networks*, vol. 15, no. 3, April 2009, pp. 279–294.
[10] J. D. Gibson, A. Servetti, H. Dong, A. Gersho, T. Lookabaugh, and J. C. De Martin, "Selective Encryption and Scalable Speech Coding for Voice Communications over Multi-Hop Wireless Links", In *Proc. IEEE MILCOM 2004*, vol. 2, 2004, pp. 792–798.
[11] S Lindskog, J. Strandbergh, M. Hackman, and E. Jonsson, "A Content-Independent Scalable Encryption Model", *Computational Science and Its Applications–ICCSA 2004*, LNCS 3043, 2004, pp. 821–830.
[12] W. Wang, S. C. Liew, and V.O. K. Li, "Solutions to performance problems in VoIP over a 802.11 wireless LAN", *IEEE Transactions on Vehicular Technology*, vol. 54, 2005, pp. 366–384.
[13] H. Dong, J. D. Gibson, and M. G. Kokes, "SNR and bandwidth scalable speech coding", In *Proc. of IEEE ISCAS 2002*, vol. 2, 2002, pp. 859–862.
[14] B. Vaidya, D. Y. Choi, J. A. Park, and S. J. Han, "Multipath Routing Scheme for Wireless Multihop Network", *Computational Science and Its Applications - ICCSA 2008*, LNCS 5073, vol. 2, 2008, pp. 433–445.
[15] L. R. Reddy, and S. V. Raghavan, "SMORT: Scalable multipath on-demand routing for mobile ad hoc networks", *Elsevier Ad hoc Networks Journal*, vol. 5, no. 2, 2007, 162–188.
[16] B. Vaidya, S. S. Yeo, D. Y. Choi, and S. J. Han, "Robust and Secure Routing Scheme for Wireless Multihop Network", *Springer Personal and Ubiquitous Computing*, 2009.
[17] OPNET Modeler homepage, [Online]. Available: http://www.opnet.com.

978-1-4244-4148-8/09/$25.00 ©2009