International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 2, Issue 12 (December 2013) PP: 65-72

Protected Direction-Finding and Information Broadcast in Portable Networks

Dr.M.S.Satish Babu[1], Mr.G.Rajasekhar Reddy[2], Mr.A.Hariprasad Reddy[3].
[1]Professor,Computer Science Department, CMR Engineering College, Hyderabad
[2]Associate professor,Computer Science Department, CMR Engineering College, Hyderabad
[3]Assistant professor,Computer Science Department, CMR Engineering College, Hyderabad

Abstract: In this paper, we exhibit a character (ID) based convention that secures AODV and TCP with the goal that it can be utilized as a part of element and assault inclined situations of portable impromptu systems. The proposed convention secures AODV utilizing Sequential Aggregate Signatures (SAS) taking into account RSA. It additionally produces a session key for every pair of source-destination hubs of a MANET for securing the end-to-end transmitted information. Here every hub has an ID which is assessed from its open key and the messages that are sent are validated with a mark/MAC. The proposed plan does not permit a hub to change its ID all through the system lifetime. Subsequently it makes the system secure against assaults that objective AODV and TCP in MANET. We introduce execution investigation to approve our case.

Keywords: manet,aodv,tcp,signature,attacker,security

I. INTRODUCTION

A mobile ad hoc network (MANET) is a gathering of two or more hubs outfitted with remote interchanges and systems administration capacity. The hubs inside the radio reach can promptly speak with each other. The hubs that are not inside each other's radio extent can speak with the assistance of moderate hubs where the parcels are transferred from source to destination. Every hub ought to be arranged with a remarkable character to guarantee the parcels accurately directed with the assistance of a steering convention of a MANET.

MANETs have particular favorable circumstances over customary systems: (an) it can be effortlessly set up and disassembled; (b) it is a savvy answer for giving correspondence in regions where setting up settled foundations is not a reasonable alternative imperatives, for example, land area, monetary ramifications, and so forth; (c) it can be set up in crisis circumstances (e.g., salvage mission). A hub requires verification for secure data trade and to maintain a strategic distance from the security dangers. Nonetheless, setting up secure correspondence in a MANET is especially testing errand as a result of the accompanying issues: (a) mutual remote medium; (b) no unmistakable line of protection; (c) self-arranging and element system; (d) the majority of the messages are telecasted; (e) messages go in a bounce by-jump way; (f) hubs are compelled as far as calculation and battery power. In this paper, we concentrate on the issue of secure course disclosure and information transmission in a free MANET.

Steering conventions in a MANET can be characterized into three classes in view of the fundamental directing data redesign component utilized: receptive (on-interest), proactive (table driven) and cross breed. In responsive directing conventions, hubs discover courses just when they should send information to the destination hub whose course is obscure. Impromptu On-interest Distance Vector (AODV) [1] and

Dynamic Source Routing (DSR) are under this classification. Then again, in proactive conventions, for example, Destination Sequenced Distance Vector (DSDV), hubs intermittently trade topology data, and henceforth hubs can acquire course data whenever they should send information. Crossover steering conventions like zone directing convention (ZRP) consolidate the best elements of both responsive and proactive directing conventions. Every hub utilizes proactive steering conventions to achieve hubs inside certain topographical (zone), and receptive directing conventions for the rest. The responsive steering conventions are observed to be more effective in a powerfully changing topology like MANET. Under receptive directing, AODV is the most prominent and is at present being looked into effectively. Web designing team (IETF) has made AODV as the standard steering convention for MANET [2]. Along these lines, in this paper we have researched and proposed enhancements in AODV directing convention.

AODV is a receptive convention that gives course on interest premise between hubs effectively. It surges the course ask for (RREQ) message all through the system at the season of course disclosure process. Along these lines, the RREQ message achieves the destination hub and responds with a course answer message (RREP). The RREP is sent as a unicast, utilizing the way towards the source hub set up by the RREQ. After the fruitful course revelation process, information parcels can be conveyed from the source to the destination hub and the other way around. Notwithstanding, it doesn't give any confirmation or information security component.

Therefore taking after are the security dangers [3] that are connected with AODV:

- Attacks utilizing alteration
- **Redirection by Altering the Course Grouping Number:** AODV utilizes monotonically expanding arrangement numbers to find and keep up the courses for a destination. A noxious hub may divert the movement through itself by publicizing with a higher destination arrangement number than the real one.
- **Redirection by Altering the Jump Tally:** As AODV uses the bounce check field to decide a most brief way, a malignant hub may occupy the movement through itself by resetting the bounce tally quality to a littler worth.
- **Denial-of-Administration by Adjusting Source/Destination:** A disavowal of-administration assault can be propelled in AODV by changing the source or destination location of a parcel. Accordingly, movement might be dropped, diverted to an alternate destination or to a more drawn out course to reach to destination that causes superfluous correspondence delay.
- **Tunneling:** In a burrowing assault, two or more pernicious hubs may work together to exemplify and trade directing messages between them along existing information courses. Subsequently, the destination hub dishonestly trusts that the most brief course from the source is through these working together hubs and wrongly sets the way through them.
- Impersonation assaults In this assault, a pernicious hub changes its personality, (for example, IP location or MAC location) to an approved hub in the friendly parcels. The making trouble hub can change the topology of the system or segregate any approved hub from the system.
- Attacks utilizing creation
- **Falsifying course blunder message:** AODV executes way support to recoup broken ways when hubs move. On the off chance that the destination hub or a halfway hub along a dynamic way moves, the hub upstream of the connection break sends a course blunder message along the opposite way toward the source hub. A malevolent hub may send false course mistake message to the source hub. Subsequently, the source hub re-starts the course disclosure process by television a course ask for message.

As of late, various secure steering conventions have been proposed [2]–[7]. Be that as it may, secure steering conventions alone guarantee the accuracy of the course revelation, can't promise secure information conveyance at transport layer of the convention stack. An astute aggressor can conceal itself at the season of course revelation to place itself on a course. Later it can begin dropping, producing, misrouting and infusing of information parcels. Transmission Control Protocol (TCP) is one of the vehicle layer convention which gives end to-end association, dependable conveyance of information parcels, stream control, clog control and end-to-end association end. Notwithstanding, it can't give any security instrument and taking after are the assaults [8] in this layer can be found in MANET:

- **SYN Flooding Assault:** In SYN flooding assault, an assailant makes countless opened TCP associations with a casualty hub yet never finishes the handshake to completely open the association. Amid SYN flooding, the assailant sends a lot of SYN bundles to the objective hub, satirizing the arrival location of the SYN parcels. At the point when the objective machine gets the SYN bundles, it conveys SYN-ACK parcels to the sender and sits tight for ACK bundle. The casualty hub stores all the SYN bundles in a settled size table as it sits tight for the affirmation of the three-way handshake. These pending association solicitations could flood the support and may make the framework inaccessible for long time. Figure 1 (a) demonstrates the typical association foundation utilizing three-way handshaking (when hub M acts ordinarily) and SYN flooding assault (when hub M carries on perniciously).

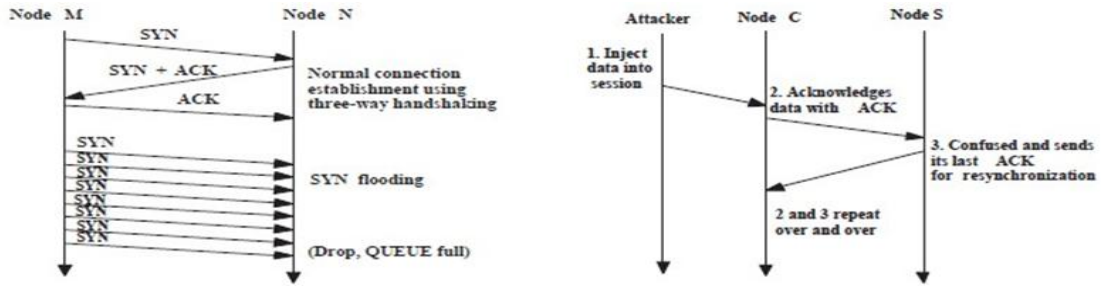

Fig. 1. (a) Normal connection establishment using three-way handshaking and SYN flooding attack; **(b)** ACK Storm.

- **Session Hijacking:** All the correspondences are verified just toward the start of session setup. The aggressor may exploit this and submit session capturing assault by satirizing the IP location of target machine and deciding the right grouping number. In this way it plays out a DoS assault so that the objective framework gets to be inaccessible for a specific timeframe. The aggressor can now proceed with the session with the other framework as a true blue framework.

- **ACK Storm:** The aggressor dispatches a TCP session capturing assault toward the starting and it then sends infused session information to hub C. Hub C then recognizes the got information with an ACK bundle to hub S. Hub S is befuddled as the bundle contains a startling grouping number. In this way, it tries to re-synchronize the TCP session with hub C by sending an ACK parcel that contains the proposed grouping number. Be that as it may, the strides are taken after over and over and results in TCP ACK storm which is appeared in Figure 1 (b).

In this paper, we propose an ID based Secure AODV that safely finds and keeps up the course. In our work we have expected two levels of security: high and low. By abnormal state of security we imply that, when a way is set up, both the source and the destination hub checks the legitimacy of the various hubs in the course. Notwithstanding this, the realness of a hub is likewise checked by its quick downstream hub. If there should arise an occurrence of low level of security, when a way is set up the source and destination hub confirms the realness of each (flip side to-end) and every transitional hub on the course checks the validness of the downstream hub. What's more, we propose an ID based secure TCP that safely transmits information utilizing the Diffie-Hellman [9] session key for the MANET hubs. In the proposed plan, every hub has an ID which is assessed from its open key for confirmation reason. Taking after the proposed plan a hub can't change its ID all through the lifetime of the MANET. In this manner, the plan is secure against the above assaults that are connected with AODV and TCP in MANET.

II. RELATED WORK

For giving security in MANET, the primary targets are to make the steering convention secure and to ensure transmitted information. In any case, these are especially trying for MANETs with powerfully evolving topologies. Taking after plans are proposed in the writing to secure the steering convention and information transmission of TCP.

Hu et al. [4] have proposed Ariadne, a protected on-interest specially appointed steering convention in light of DSR that averts aggressors or bargained hubs utilizing the symmetric cryptography. To persuade the objective of the authenticity of every field in a course demand, the initiator essentially incorporates a message validation code (MAC) in the solicitation. The objective can undoubtedly confirm the credibility and freshness of the course ask for utilizing the common key. One-way hash capacities are utilized to confirm that no bounce was discarded which is called per-jump hashing. Three option procedures to accomplish hub list validation: the TESLA convention [10], advanced marks, and standard MACs.

Secure Routing Protocol (SRP) [5] utilizes symmetric cryptography to give end-to-end confirmation. The convention depends on course questioning strategy and it requires a Security Association (SA) amongst source and destination hub. The security affiliation is acquired by means of the information of the correspondence partner's open key. SRP makes no suspicion with respect to the middle of the road hubs, which displays discretionary and malevolent conduct. Hubs use secure message transmission (SMT) [11] to guarantee effective conveyance of information bundles.

The Authenticated Routing for Ad hoc Networks (ARAN) [3] depends on AODV and it is a stand-alone convention that uses cryptographic open key testaments marked by a trusted power, which relates its IP address with an open key keeping in mind the end goal to accomplish the security objectives of verification and non-denial. ARAN utilizes cryptographic declarations to bring confirmation, message-trustworthiness and non-renouncement to the course disclosure process. The source hub telecasts a marked course disclosure bundle (RDP) to its neighbors for a course to the destination. The RDP incorporates a bundle sort identifier, the location of the destination, declaration of the source hub, timestamp and a nonce. A middle of the road hub utilizes general society key and testament of its past hub to accept the mark of the RDP. After the acceptance, it evacuates the mark of the past hub, adds its own particular mark and endorsement. Additionally, along the answer parcel (REP) every hub expels mark of its past hub, attaches its mark and authentication before sending it to the following hub. The mark keeps malignant hubs from infusing self-assertive course revelation parcels that modify courses or frame circles.

Securing AODV (SAODV) [6] proposes an arrangement of augmentations that safe the AODV steering parcels. Two components are utilized to secure the AODV messages: computerized marks to validate the non-alterable fields of the messages, and hash chains to secure the jump check data. Since the convention utilizes unbalanced cryptography for computerized marks it requires the presence of a key administration instrument that empowers a hub to secure and check people in general key of different hubs that take part in the impromptu system.

The security issues identified with transport layer are confirmation, securing end-to-end correspondences through information encryption, taking care of postponements, bundle misfortune et cetera. The vehicle layer conventions in MANET gives end-to-end association, dependable parcel conveyance, stream control, blockage control and clearing of end-to-end association. In spite of the fact that TCP is the principle association arranged dependable convention in Internet, it doesn't fit well in MANET. TCP input (TCP-F) [12],

TCP unequivocal disappointment notice (TCPELFN) [12], specially appointed transmission control convention (ATCP) [12], and impromptu transport convention (ATP) have been produced for MANET. Be that as it may, none of them have considered the security perspective.

The plan displayed in [13] depends on perception of hub portability. In this plan, the source hub separates the message into various shares and sends the shares at various times through various halfway hubs. The destination hub joins the shares to remake the first message. Because of portability a halfway hub will most likely be unable to gather enough shares to recoup the first message. In any case, it is pertinent where postponement can be endured or the system is progressive

The SMT plan is introduced in [11] which guarantees effective conveyance of information bundles. In SMT, information messages are isolated into various bundles utilizing mystery sharing procedures and sent at the same time through numerous free courses. The destination hub effectively recreates the first message, gave that adequate shares are gotten. Every offer is transmitted alongside message verification code so that the destination can check its trustworthiness and the realness of its inception. The destination approves the approaching shares and recognizes the effectively got ones through a cryptographically secured input back to the source. Be that as it may, the plan expect that numerous ways exist in the system which may not be valid in genuine situation.

A prominent security instrument in system layer is IPSEC [14], which is utilized as a part of wired systems to alleviate the majority of the assaults examined in Section 1. IPSEC does not permit a middle of the road hub to straightforwardly get to the IP header of a transmitted parcel. Be that as it may, transport layer conventions proposed for specially appointed systems need to depend on data nourished over from the middle of the road hubs (e.g., Explicit Congestion Notification (ECN) [15]), and consequently IPSEC can't be incorporated with these conventions [16]. Comparative is the situation with SSL, PCT and TLS proposed for the most part for the wired system.

III. SYSTEM MODEL

We consider an independent specially appointed system chipping away at its own. It has no door or association with the outer world. The system is framed beginning from one hub and after that alternate hubs include one by one like IDDIP. We accept that a hub, A, have two sorts of self created RSA-based key sets: (1) open ((NA; eA))/private (dA) key pair for message confirmation/marking; (2) open (PKA)/private (SKA) key pair for message encryption/unscrambling. Here, the hub identifier IDA of hub An is created from its open key ((NA; eA)) utilizing a safe one way hash capacity (H). Thusly, a hub can't change its ID inside the lifetime of the MANET. What's more, open keys ((NA; eA) and PKA) alongside identifier IDA of every hub An are appropriated before the organization of the system so that the overhead of the proposed convention can be decrease. The private keys (dA and SKA) are kept mystery by every hub An of the system. Table I shows the documentations and their portrayals utilized as a part of this paper to depict our proposed conventions.

Table Notations and descriptions

Notations	**Description**
S, D and I	source, destination and intermediate nodes
ID_A	identifier of node A
IP_A	IP address of node A
SN_S, SN_D	sequence numbers of source and destination
$BctID$	broadcast ID
(N_A, e_A)	Public key for signature verification of node A
d_A	Private key for signature generation of node A
PK_A	Public key for encryption of node A
SK_A	Secret key for decryption of node A
K_{AB}	Session secret key shared between node A and node B
σ_A	Digital signature of node A
δ_A	Message Authentication Code tag of node A

IV. THE ALGORITHMS

As talked about in Section 2, the greater part of the RSA open key cryptography based secure steering conventions of MANET need to send a vast measured open key or authentication alongside mark in each directing message. Besides, these conventions host to depend on trusted third get-together (TTP) for the key and/or authentication conveyance to the approved hubs of the system. In this paper, we build up a RSA-based steering convention that tries to conquer these issues to an impressive degree by utilizing self-confirmation procedure. The proposed steering convention depends on AODV directing convention. We likewise watch that the protected steering conventions may not guarantee secure information conveyance at transport layer of OSI engineering. Here we additionally exhibit a method to secure the three-way handshaking procedure of Transmission Control Protocol (TCP).

We have considered two cases relying on the level of security: Case 1: High and Case 2: Low. In Case 1, i,e., for abnormal state of security (sec_ level = 1), amid steering prepare, the source and destination hubs independently check the realness of every single other hub in the way. Further, every middle of the road hub confirms the validness of its prompt upstream hub. In Case 2, i.e., for low level of security (sec_level = 0), amid steering process, both the source and the destination hubs confirm realness of each other. Additionally every hub on the way checks the validness of its prompt upstream hub from where it gets the messages (bounce by-jump).

Our proposed directing convention utilizes consecutive total marks (SAS) in view of RSA.. It has two sections: (a) safe course disclosure and session key (KAB) era; (b) secure course upkeep.

Secure Route Discovery and Session Key Generation:

***Case 1*:** When we need high level of security i.e., *sec_level* = 1, the secure route discovery procedure of the proposed protocol works as follows: to create a path between a source node *S* and a destination node *D*, the source node, *S*, first generates a prime number *p* along with two random numbers *r*1 and *g*, where *p* and *g* are publicly known parameters. *S* then computes $R1 = g^{r1}$ (*mod p*), encrypts $R2 = E_{PKD}(R1)$ broadcasts it in a signed (σS) *RREQS* message along with ID_S to its neighbours. The *RREQS* message also contains source IP IP_S, source sequence number *SNS*, broadcast ID *BctID*, and destination IP IP_D as similar to AODV protocol.

An intermediate node, *I*, on receiving the signed ($\sigma(I\text{-}1)$)*RREQ*(*I*-1) message from node (*I-1*) first checks the authenticity of the node (*I - 1*). If node (*I - 1*) is authenticated, node *I* inserts its ID ID_I and subsequently updates the *RREQI*. The intermediate node *I* also generates an aggregate signature (σI) from both *RREQI* message and the received signature ($\sigma(I\text{-}1)$). Thereafter node *I* broadcasts *RREQI* message along with the aggregate signature σI to its neighbours. This process continues till the *RREQ* message is received by the destination node.

On receiving the signed (σt) $RREQ_t$ message, the destination node *D* first checks the authenticity of all the intermediate nodes ID_t including source node *IDS* on the route. It also checks the authentication of the received aggregate signature σ_t by verifying all the signatures of node *S* to node *t*. If both checks pass, the destination *D* decrypts $R = D_{SKD}(R2)$ and generates the session key $K_{DS} = R^{r2}$ (*mod p*). It also generates a random number *r*2 and computes $R3 = g^{r2}$ (*mod p*). *D* thereafter encrypts $R4 = E_{PKS}$ (*R*3) and unicasts it in a signed (σD) $RREP_D$ message with its ID_D to *S* along the reverse direction of *RREQ* message. The $RREP_D$ message also contains other parameters of AODV (such as, source IP IP_S, destination sequence number *SND*). An intermediate node verifies the authenticity of the *RREP* message and combines its signature with the signatures of previous hops on the route in the same way as *RREQ* message. When *S* receives the signed (σt) $RREP_t$ message, it checks the authenticity of each node including *D* on the route by verifying all the *ID*s and σs. If both checks pass, *S* decrypts $R = D_{SKS}$ (*R*4) and generates the session key $K_{SD} = R^{r1}$ (*mod p*) to send the data packets to *D* via this route. Figure 2 shows an example of the route discovery process of our proposed routing protocol for *Case 1*.

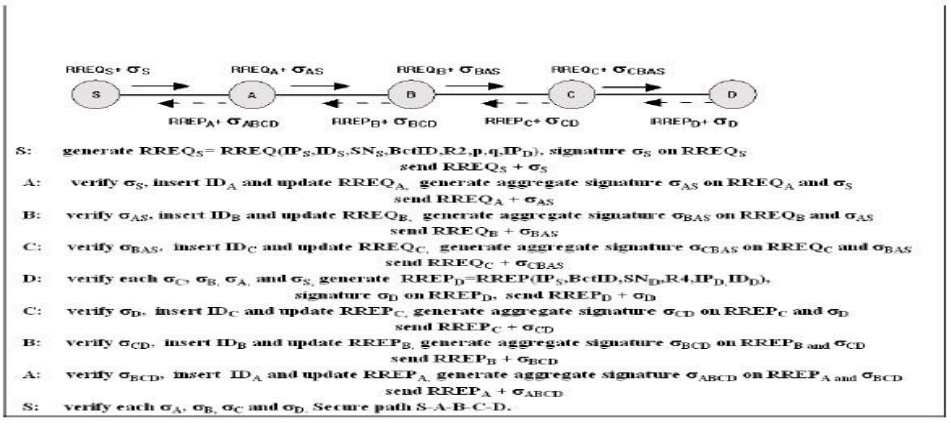

Fig. 2. An example of secure route discovery process for *Case 1*

***Case 2*:** For low security level, i.e. *sec_level* = 0, initially the source node broadcasts signed σS *RREQS* message along with its ID, *IDS*, to the neighbours in a way similar to the previous case. An intermediate node, *I*, on receiving the signed $\sigma(I\text{-}1)$ *RREQ*(*I*-1) message from node (*I-1*), first checks the authenticity of the node (*I-1*). If the node (*I-1*) is authenticated, it removes the signature of the node (*I-1*), inserts ID_I

and updates the *RREQI* message. It also generates its own signature on the *RREQI* message and the signature σ*S* of *S* and broadcasts it to its neighbours. This process continues till the *RREQ* message reaches the destination node. On receiving the signed σ*t* *RREQt* message, the destination node *D* first checks the authenticity of the node *IDt* and the source node *IDS*. It also checks the authentication of the received signature σ*t* (signature of the node *t* from whom it receives *RREQ*) and σ*S* of the source node. If both checks pass, *D* generates the session key *KDS* and unicasts the signed (σ*D*) *RREPD* message with its *IDD* to *S* along the reverse direction of *RREQ* message in the same way as in the first case. An intermediate node *I* verifies the signature σ(*I*-1) of the received *RREP*(*I*-1) message. If checks pass, it removes the signature σ(*I*-1) and ID *ID*(*I*-1), and inserts its own ID *IDI* and subsequently updates *RREPI* message. It also generates signature σ*I* on *RREPI* and the signatures σ*D* of *D*. When *S* receives the signed (σ*t*) *RREP* message, it checks the authenticity of the previous node *t* and *D* on the route by verifying the *ID* and σ of both the nodes. If both checks pass, *S* generates the session key *KSD* to send the data packets to *D* via this route. An example of the route discovery process of our proposed routing protocol for *Case 2* is shown in Figure 3.

Secure Route Maintenance: Case 1: For high level of security, i.e., *sec_level* = 1, the proposed protocol maintains a established route as follows: If a node *X* detects that its immediate down link towards *D* is broken, it sends signed (σ*X*) *RERRX* message with *IDX* along the reverse route toward *S*. On receiving a signed (σ(*I*-1)) *RERR*(*I*-1) message from node (*I-1*), an intermediate node *I* immediately checks the authenticity of the node (*I-1*) by verifying the signature σ(*I-1*) and *ID*(*I-1*).

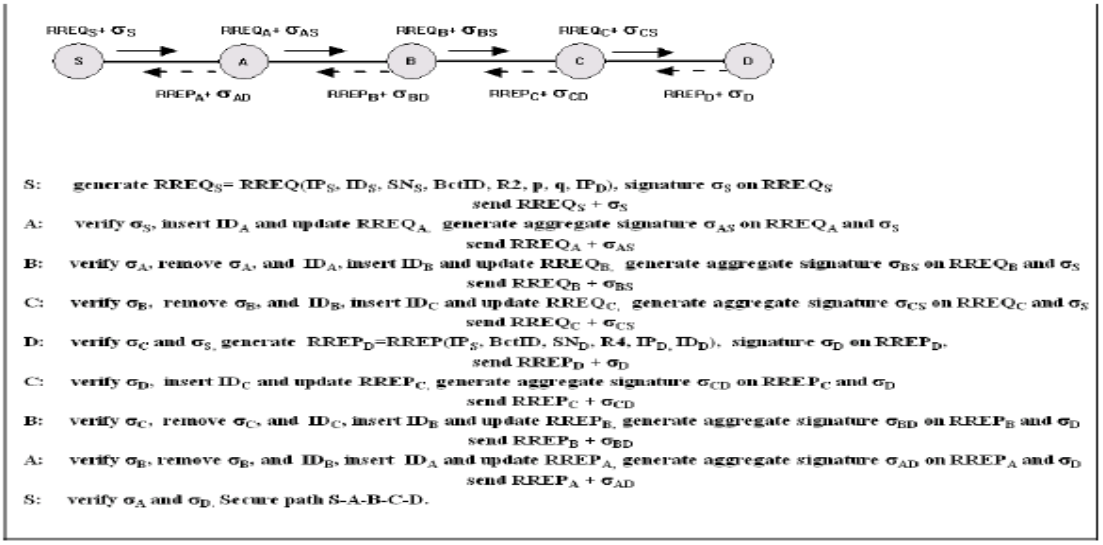

Fig. 3. An example of secure route discovery process for *Case 2*

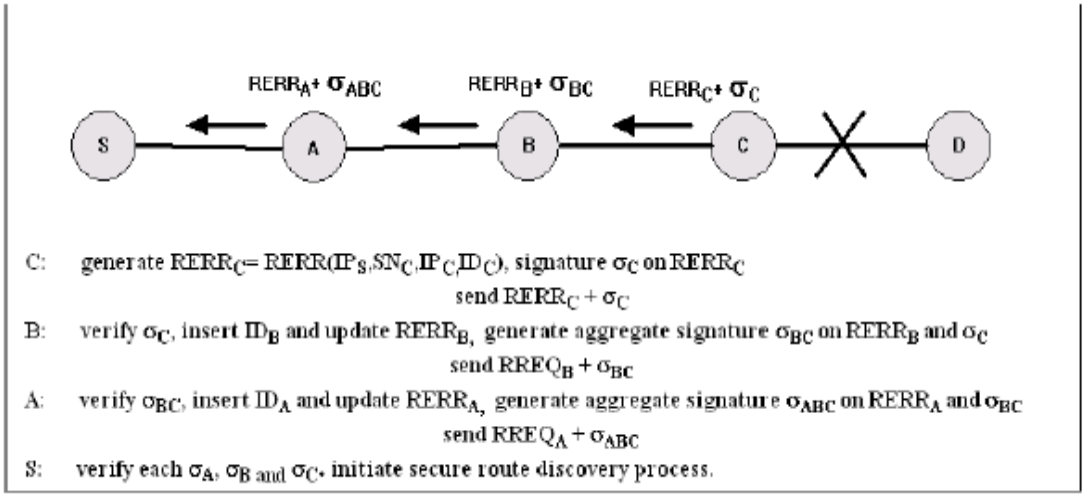

Fig. 4. An example of secure route maintenance process for *Case 1*

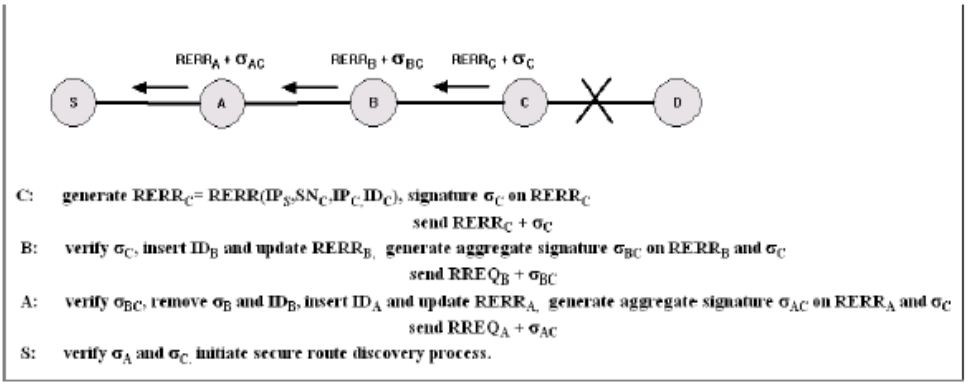

Fig. 5. An example of secure route maintenance process for *Case 2*

If node (*I-1*) is authenticated, it inserts *IDI* and updates the *RERRI* message. The node *I* also generates a signature σ*I* from the *RERRI* message and the received signature σ(*I-1*) and forwards the signed σ*I* *RERRI* message along the path toward *S*. On receiving the σ*t* *RERRt* from *t*, *S* verifies all the signatures and *ID*s of the nodes on the route. If both verifications pass, *S* initiates the route discovery process of our proposed routing protocol. The secure route maintenance process for *Case 1* of our proposed routing protocol is given by an example in Figure 4.

Case 2: For low level of security, i.e., *sec_level* = 0, the route maintenance of the proposed protocol works as follows: After detecting the connection loss, node *X* sends signed (σ*X*) *RERRX* message with *IDX* along the reverse path toward *S*. On receiving the signed (σ(*I-1*)) *RERR*(*I-1*) message from node (*I - 1*), an intermediate node *I* first checks the authenticity of the node (*I - 1*) by verifying the signature σ(*I-1*) and *ID*(*I-1*). If the node (*I - 1*) is authenticated, it removes *ID*(*I-1*) and updates the *RERRI* message by appending *IDI*. It also generates the signature σ*I* on the *RERRI* message and the signature σ*X* of node *X*. Node *I* forwards the signed σ*I* *RERRI* message along the path toward *S*. On receiving the σ*t* *RERRt* from *t*, *S* verifies the signatures σ*t*, σ*X* and *IDt*, *IDX*. If both verifications pass, *S* initiates the route discovery process. The secure route maintenance process for *Case 2* of our proposed routing protocol is shown by an example in Figure 5. The algorithm for secure route maintenance process of our proposed routing protocol is given in Algorithm 4.

Secure Data Transmission

As discussed in the previous Section 4, after discovering the secure path, source and destination node have common session secret key (i.e., K_{SD}= K_{DS}). Initially source node (*S*) starts connection establishment with destination node (*D*) using three-way handshaking of TCP. *S* at first generates the initial sequence number (ISN_S) from a random number (*R*) and a hash function of source port, destination port, ID_S, ID_D and session secret key K_{SD}. Subsequently, it generates authentication tag (δ_S) on *SYN*(ISN_S) segment using HMAC function and K_{SD}, sends it to *D* along with *SYN*(ISN_S) segment. On receiving the *SYN*(ISN_S) + δ_S, *D* generates the authentication tag (δ_G) from the received *SYN*(ISN_S) and K_{DS}. If the generated tag (δ_G) and received tag (δ_S) are same, *S* is authenticated to *D*. At this point *D* also generates the initial sequence number (ISN_D) and authentication tag (δ_D) on *SYN*(ISN_D) + *ACK*(ISN_S+1) segment in a way similar to *S*, and sends it to *S* along with the segment. On receiving *SYN*(ISN_D) + *ACK*(ISN_S+1) + δ_D, *S* generates the authentication tag (δ_G) on *SYN*(ISN_D) +*ACK*(ISN_S+1) segment and matches the generated tag (δ_G) with the received tag (δ_D). If both are same, *D* is authenticated to *S*, and *ACK*(ISN_D+1) + δ_S segment is sent by *S*. *D* generates the authentication tag (δ_G) on the received *ACK*(ISN_D+1) segment and checks it with the received tag (δ_S). If the tags match, *S* is authenticated. This completes the three-way handshake process and therefore *D* allocates the resource for *S* to start transmission of data along with the authentication tag.

The algorithms for the three-way handshake connection establishment process for source (*S*) and destination (*D*) nodes are given in Algorithm 5 and Algorithm 6 respectively. Figure 6 shows a schematic for a secure three-way handshaking connection establishment process of our proposed protocol using a timing diagram.

The above process is followed to secure the three-way handshake connection termination process too. Session key K_{SD} terminates after the end of one session or at any stage if authentication fails in the three-way handshake process. For a new session, a new key is obtained at the time of route discovery and the process is repeated.

V. CONCLUSION

In this paper the popular MANET routing protocol AODV and the standard TCP has been improved and made suitable for using it in mobile ad hoc networks. The proposed routing protocol provides security to the route discovery and route maintenance phases. Further, the three-way handshaking process of standard TCP has been secured. Here each node is made to have an *ID* that is generated from its public key and is unchangeable throughout the lifetime of the network. Performance analysis shows that our proposed protocols are secure against the attacks that are associated with AODV and TCP in MANET.

REFERENCES

[1] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," draft- ietf-manet-aodv-11.txt, June 2002 (work in progress).

[2] J. Kim and G. Tsudik, "Srdp: securing route discovery in dsr," in Mobile and Ubiquitous Systems: Networking and Services, pp. 247–258, July 2005.

[3] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in Proceedings of 10th IEEE International Conference on Network Protocols and ICNP'02, pp. 78–87, IEEE Computer Society, 2002.

[4] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in Proceedings of the 8th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '02), September 2002.

[5] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 27-31 2002.

[6] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2002.

[7] U. Ghosh and R. Datta, "Sdrp: Secure and dynamic routing protocol for mobile ad hoc networks," IET Networks, 2013 (Accepted).

[8] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in Wireless Network Security, Springer US, 2007.

[9] W. Diffie and M. E. Hellman, "New directions in cryptography," in IEEE Trans. Inf. Theory, vol. IT- 22, pp. 644–654, November 2006.

[10] A. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient and secure source authentication for multicast," in Proceedings of Network and Distributed System Security Symposium and NDSS'01, pp. 35–46, February 2001.

[11] P. 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, pp. 343–356, 2006.

[12] H. Hsieh and R. Sivakumar, "Transport overwireless networks," in Handbook of Wireless Networks and Mobile Computing, Edited by Ivan Stojmenovic. John Wiley and Sons, 2002.

[13] Q. Zheng, X. Hong, J. Liu, and L. Tang, "A secure data transmission scheme for mobile ad hoc networks," in Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), pp. 1006 –1010, November 2007.

[14] "Ip security protocol (ipsec)." http://www.ietf.org/html.charters/ipsp-charter.html.

[15] K. K. Ramakrishnan, S. Floyd, D. Black, and G. K. Ramakrishnan, "The addition of explicit congestion notification (ecn) to ip," 2001.

[16] R. de Oliveira and T. Braun, "Tcp in wireless mobile ad hoc networks," tech. rep., 2002.

[17] R. P. C. Kaufman and M. Speciner, "Network security private communication in a public world," in Handbook of Wireless Networks and Mobile Computing, Prentice Hall PTR.