Journal of Computer Science 9 (5): 607-619, 2013
ISSN 1549-3636
© 2013 Science Publications
doi:10.3844/jcssp.2013.607.619 Published Online 9 (5) 2013 (http://www.thescipub.com/jcs.toc)

Protocols for Secure Routing and Transmission in Mobile Ad Hoc Network: A Review

[1]Salwa Aqeel Mahdi, [1]Mohamed Othman, [1]Hamidah Ibrahim, [2]Jalil Md. Desa and [3]Jumat Sulaiman

[1]Department of Communication Tech and Network,
Faculty of Computer Science and Information Technology, University Putra Malaysia, Malaysia
[2]Telekom Research and Development, TM Invoation Center, Malaysia
[3]School of Science and Technology, Mathematics with Economics, University Malaysia Sabah, Malaysia

Received 2012-11-22, Revised 2012-12-30; Accepted 2013-05-25

ABSTRACT

Mobile ad hoc network security is a new area for research that it has been faced many difficulties to implement. These difficulties are due to the absence of central authentication server, the dynamically movement of the nodes (mobility), limited capacity of the wireless medium and the various types of vulnerability attacks. All these factor combine to make mobile ad hoc a great challenge to the researcher. Mobile ad hoc has been used in different applications networks range from military operations and emergency disaster relief to community networking and interaction among meeting attendees or students during a lecture. In these and other ad hoc networking applications, security in the routing protocol is necessary to protect against malicious attacks as well as in data transmission. The goal of mobile ad hoc security is to safeguard the nodes' operation and ensure the availability of communication in spite of adversary nodes. The node operations can be divided into two phases. The first phase is to discover the route (s) path. The second phase is to forward the data on the available discovered routes. Both stages need to protect from attacks; so many protocols have been proposed to secure the routing and data forwarding. This is a review study to mobile ad hoc protocols for securing routing as well as protocols for securing packets forwarding. Furthermore, it will present the characteristics and the limitations for each protocol and attributes.

Keywords: Securing Routing, MANET Security, Passive Attack, Reactive Attack, Security Forwarding

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is defined as a network without infrastructure, meaning a network without the usual routing infrastructure like fixed routers and routing backbones. It composes of a number of nodes that connect on wireless medium with each other in a specified range zone. Since the wireless medium zone is limited the node forwards a packet either by one hop or using multiple hops when the destination out of the zone as illustrated in **Fig. 1**. There are many applications depending on using MANET such as military mission, relief disaster and meeting. Some of these applications provide sensitive and significant information that must be secured from unauthorized accesses for confidential information. This illegal access is considered as an attack. Attacks can be divided into two types: Passive Attack and Active Attack (Komninos *et al*., 2007).

Passive attack is eavesdropping on transmission and it is difficult to detect. While active attack involves modifying or creating a fraudulent stream. Unfortunately, all types of MANET protocols have no security and can be easy vulnerable to any types of attacks.

Corresponding Author: Salwa Aqeel Mahdi, Department of Communication Tech and Network,
Faculty of Computer Science and Information Technology, University Putra Malaysia, Malaysia

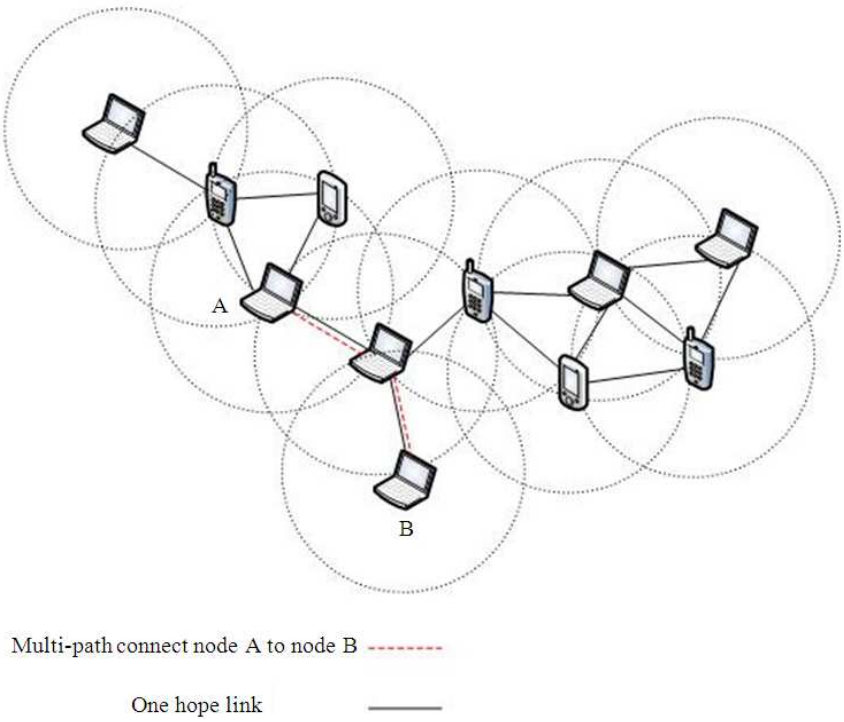

Fig. 1. Mobile ad hoc network

To face these attacks many new security protocols have been appeared to remove these endangered attacks and obtained MANET securities.

The malicious nodes that have reactive attack acting can be treated by using some security protocols that they are involved some type of cryptographic methods. These security protocols have to satisfy some of the objectives, which are (Anjum and Mouchataris, 2007):

- Confidentiality: It ensures that information content is hided to unauthorized entities
- Integrity: It ensures that data is not modified during transmission
- Authentication: It ensures a node of the identity of the other party or parties that it is communicating with
- Non-repudiation: Guarantees that a party cannot be false denying its action
- Availability: It ensures that the network services are available

Since there are many attacks require defining them. It is difficult to have a universal protocol that can satisfy all the above security objectives. There are many protocols appeared to secure Mobile Ad Hoc routing and packet forwarding that it is focused on different types of the attack.

Mobile Ad Hoc Networks communication has two phases, route discovery and data transmission. Both phases are vulnerable to a variety of attacks. The main goal of this study is to show introductory to the different types of attack, securing routing and of forwarding packets protocols.

1.1. Mobile Ad Hoc Attacks

There are two types of attacks passive and active. The passive attack does not change data packets or modify any operations for control packets. It is only overheard to the packets during transmission without modify them. An attacker requires being within radio range of a node to listening. Here the attack aims the confidentially requirement. The discovering of this attack is very difficult due to it is not changing anything. One solution for this attack is to use potent encryption methods to encrypt the data need to transmit.

In active attack, the adversary node intervenes against the operations of the network. This attack can affect the network routing path, reading either by altering the routing data, hop count, spoofing another node IP and other.

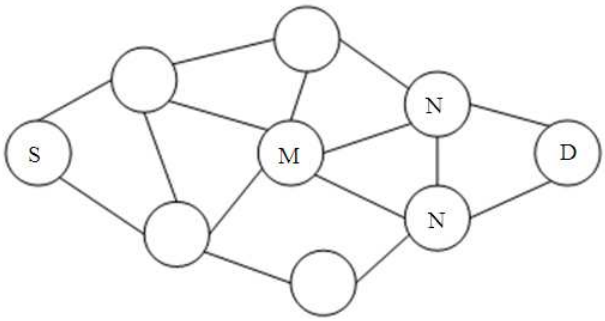

Fig. 2. Example of network describing rushing attack

While in the forward packet, this attack is done either by drop the packet, reading and modifying the packets. The detection of active attack is easy since it made some alteration to the network function. The following describes briefly some types of active attack.

1.2. Black Hole Attack

Black hole attack is an attacked node cooperated well in the route discovery, but it is dropped the packet while forwarding it. In route discovery the black hole node all the time gives the correct responds to route request and route reply. Nevertheless, it does not have a path to the destination node. When the source node forwards the data packet, this node discarded the data packet and makes a hole in the path that denied any packets transmit. There are two types of black hole: Single Back Hole (Deng *et al*., 2002) and Multiple Black Hole (Ramaswamy *et al*., 2003). In Single Black Hole attack, one node pretended had the shortest path to the destination. The black hole node when engage in the routing, it performs denial of service or drops the forward packets. In Multiple Black Hole attack two nodes or more cooperate to misrepresent the existence of a path to the destination. Two solutions for Single black hole attack are suggested in Al-Shurman *et al*. (2004). One solution is done by receiving repeated reply at the source. The source selects a route path that has repeated portion with another route path. In the second solution, each node constructs two tables to keep sequence numbers of the packets. The first table consists of sequence numbers of the last packet sent to other nodes. While the second table is comprised of sequence numbers received from other nodes. In reply phase, each node required to match the sequence number of the packet received with a sequence number in the table to verify the correctness of the reply packet. Ramaswamy *et al*. (2003) proposed a solution for Multiple Black Hole attack by using an additional table Data Routing Information (DRI) to provide nodes reliability to and cross checking algorithms to check node reliability and find the cooperative black hole nodes.

1.3. Rushing Attack

It is an unfamiliar attack, in which the attacker attempts to be part of routing path to cause the denial of service attack. The attack is directed to reactive protocol only. This attack exploits the property that each node processes just the route request packet for specified identity once.

When rushing attack launched during the route discovery, only a route not longer than two hops is found. As shown in **Fig. 2** the source S starts by forward packet to the destination D. The malicious node M when received the route request to D it quickly broadcasts the request to one of the destination neighbor N without any checking for request demand. Finally, the destination received the request from N. So this route request is selected and other discards since each node must process one route request. Tamilselvan and Sankaranarayanan (2006) is suggested a solution to rushing attack. The nodes instead of relay the first route request packet received, they select arbitrarily the relayed packets. Another solution is proposed by designing a new protocol called Rushing Attack Prevention (RAP) (Hu *et al*., 2003c). Rushing Attack Prevention (RAP) selects the forward request randomly after verifying it sends from a node within it is a neighbor rang.

1.4. Jellyfish Attack

In this attack, the attacker attempts to degrade the performance of the network. Firstly, the attacker node requires participating in the route path. Secondly, it is delays' transmission of the data packet to increase end to end delay. This particular attack was first introduced by Imad *et al*. (2004) with three scenarios which aimed to reduce performance near zero. The detection of jellyfish attack is very hard; due to the attacker, node complies with the routing and forwarding requirement.

1.5. Wormhole Attack

In the wormhole attack, two nodes cooperate to construct a tunnel between them. This tunnel is built either by using wire cable, wireless transmission or any media (Hu *et al*., 2003d; Maheshwari, 2007).

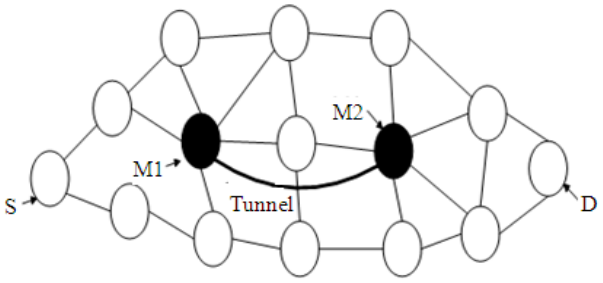

Fig. 3. Explanation of a Wormhole Attack, M1 and M2 denotes the wormhole nodes connected through the tunnel link

In **Fig. 3** two nodes overcome any packet transmission through the tunnel they established. The original node of the tunnel sends the packet to the destination of the tunnel to replay them. The attack is succeeded even with strong cryptography methods due to the lack of doubt to any node, or lack of disrupt the integrity and authentication of the packets. Once the wormhole attack is released, it can cause dropping or altering the data packets. Furthermore, it can present fault network connectivity. Many techniques attempt to recover from this attack (Hu *et al*., 2003d; Sanzgiri *et al*., 2002) either by using time based methods, or revealing location information.

1.6. Securing Routing Discovery Protocols

In the securing routing protocols the routes discovered between the source and destination must be protected from any malicious nodes attempt to forge, fabricated, disrupted the route and replayed. There are two classes of routing protocols exist in the MANET world. The first class, reactive protocols acquire routes on demand through flooding a route request and receiving a route reply. The other class of MANET routing protocols is proactive; it ensures that all nodes at all times have sufficient topological information to construct routes for all destinations in the network through periodic message exchange.

1.7. Secure Routing Protocol (SRP)

Secure Routing Protocol (SRP) can be applied as an extension of Dynamic Source Routing (DSR) protocols (Papadimitratos and Haas, 2002; Papadimitratos *et al*., 2002; Papadimitratos, 2005). The requirement for SRP protocol is the existence of a Security Associated (SA). It applied security associated only at the end nodes and no need for any cryptographic methods at intermediate nodes. For each route request (as well as reply), SRP used two numbers to identify the request to improve the security; one is a sequence number that is increased periodically. The other one is a random Identifier. In addition, the header of SRP maintains Request Message Authentication Code (MAC). The MAC field is generated by a key hash algorithm, which its input is the entire IP header, the route request packet and the shared key. Two MAC fields are generated by the source for the request packet and by the destination for the reply packet to verify the authentication of packets from the original nodes. SRP guarantees the discovery of correct connectivity information in the presence of malicious nodes. The only possible attacks against the protocol would be if two or more nodes colluded during single route discovery and middle man attack.

1.8. Ariadne

Ariadne applies security protocol above on-demand routing protocols for ad hoc networks (Hu *et al*., 2005; Hu and Perrig, 2004). It can authenticate routing messages using TESLA. TESLA is an efficient authentication method that achieves an asymmetry protocol from clock synchronization and delayed key disclosure, rather than from computationally (Perrig *et al*., 2000; 2001). This protocol needs synchronization methods since the authentication is done using clock time. The evaluation for this protocol is done by comparing Ariadne to a version of Dynamic Source Routing protocol (DSR). The result shows the overhead of Ariadne was higher than for DSR, due to the overhead of the authentication information in Ariadne's routing packets. However, for the other matrices Ariadne has about the same on all other metrics.

1.9. Trust-Aware Routing Protocol (TARP)

TARP is a new proposed protocol idea (Abusalah *et al*., 2006). It is building as part of routing protocol not like another security protocol that would be added as a new layer to the routing protocol. The TARP secures trusted routing that is done by evaluating the trust level of its neighbours using attributes. These attributes are battery power and software configuration. In this protocol when a route path is selected the selection must be not considered only the shortest path factor but also the nodes' power factor (battery power). The software configuration means that the sender has the right to select which secure route might utilize to send data. The protocol is modified the packet format for the RouteRequest by adding two bits for each attributes.

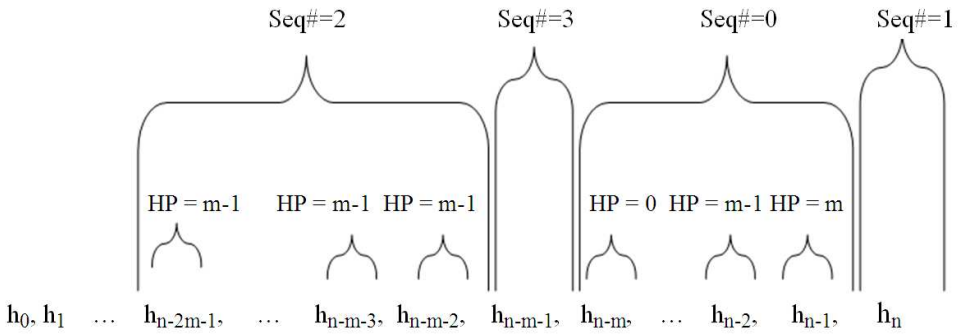

Fig. 4. Hash chaining structure

These two bits specified the four levels that the sender can select from it. Most of the protocol focuses on confidence and integrity security requirements, but TARP focuses on security availability (that the network resources are available all the times to keep the connection stable). The performance evaluation of TRAP that applied to DSR shows' improvement to the network availability and reduces the routing traffic sent and received.

1.10. Secure Multipath Routing Protocol (SecMR)

The Secure Multipath Routing (SecMR) protocol (Mavropodi *et al*., 2006) is on-demand multipath routing protocol. SecMR discovers the complete non-cyclic and node-disjoint paths between a source and a target node. The protocol works in two phases: neighborhood authentication phase and route discovery and maintenance phase. In neighborhood authentication phase each node has a pair of public secret key. The public key of each node is certificate using Certifying Authority (CA). The route discovery and maintenance phase compose of three methods. The route request used to discover multipaths; the route reply is used to forward the routing paths and the route error is used to update a broken. The protocol used ExcludeList field in route request query, which is a list of nodes excluded from the route discover query; and NextHop field, is the list containing the nodes that are allowed to be the next hop (node neighbors that will be used in the next RouteRequest). SecMR maintains keyed hash function to check the validity of the fields of the route request.

1.11. Secure Dynamic MANET On-Demand (SEDYMO)

This protocol is an expansion to the reactive protocol DYMO (Dynamic MANET On-demand) (Chakeres and Perkins, 2007). To enforce security to DYMO, hash chain and digital signature is required (Helena and Jordi, 2007). The hash chain is to ensure the number of hopes (mutual field) that the route request traverse is not altered by any malicious node. To validate the non mutual fields and authentication of the packets a digital signature is used. A distributed Certificate Authority is required to apply certificates to each node. Each intermediates node has to check the signature of the packet is correct and the hash chain for the hopes' number is right. Then the node adds it is signature and increase hope count and hash the hash value after that it can broadcast the packets to next neighbors. For Error message, a signature is added to verify the node that constructs the Error message. Since the secure protocol builds with asymmetric cryptography, there is a high overhead in the routing operation. Moreover, the problem of central authentication is difficult to construct in mobile ad hoc.

1.12. Secure Efficient Ad hoc Routing Protocol (SEAR)

The SEAR (Li *et al*., 2008) is a secured protocol for an Ad hoc On-Demand Vector protocol (AODV). AODV request packet has two main fields need to be secure: the sequence number of the request and the hop number. To secure these two fields, SEAR uses symmetric cryptography for authentication them and asymmetric cryptography in the bootstrap phase to broadcast the authentication vow. Each node generates two authentication hash chains, one to protect the sequence number and the hope number. **Figure 4** shows the structure of the hash chain where n+1 is the chain length, m is the maximum number of hopes, Seq# means the sequence number and the Hp denotes the hope number. The second chain uses TESLA chain to protect the Error packets. In the hash chain generator, even sequence numbers use to authenticate the route Request and Reply packets. For the Error packet, the odd

sequence number of the chain is exploited to authenticate it. One of the SEAR problems is the distribution of the authentication vows. The second problem requires all the nodes are loosely time synchronized to apply TESLA. Furthermore, if the hash chain is long and the sequence numbers high, then a lot of computations for verify the sequence number and hop number.

1.13. Multilevel Secure Ad Hoc On-Demand Routing (MOSAR)

This protocol (Hongwei and Atam, 2010) is built by classify the nodes to different level of security either in DSR or ADOV protocol. It adds a new field to the header of the packet called Security Requirement. The packet with the specified security level can pass the packet to all paths from a node equal or a lower security level. It thus means the packet with more security requirement packets have higher security performance and more power consuming. In this protocol, the authentication is done depend on the security requirements of the packet. If the security requirement high a digital signature can be used since, the power consuming is not a problem. In other hands when the packet has low security requirements, a Message Authentication Code (MAC) is applied. The problem of this protocol needs an Authentication centre to build the classification of security levels.

1.14. Appalls

APPALLS (Kulasekaran and Ramkumar, 2011) is secured routing protocol founded on DSR. It is similar to Ariadne, but it concentrates on the monitor strategy. The monitor is appended to route around misbehaving nodes. The route request use shared key between the source and destination for authentication the original of the packet. However, a group key is used to authenticate the broadcast packet among neighbor nodes in the network. Every node joins the network has to get a private and public key from a server for signature and authentication purpose. For monitor strategy, each node will have to detect its neighbors' nodes by send a prop packet and negotiated between them to build a key group. This group key is used by specified node to send and rely on packet to other nodes in the group. That means, every node enforces a Private Logical Neighborhood (PLN) (Sivakumar and Ramkumar, 2008) which it is a subset of nodes in the reliable delivery neighborhood. When any node in the group suspect of a selfish node manner, the node cuts off the suspend node from the PLN. A new group is cons trusted with fresh group key. APPALLS is a modern protocol compounded security with reputation. Although it is still can face wormhole attack.

1.15. An Efficient Secure Routing Protocol (ASRP)

Nabet *et al*. (2011) suggests a secured protocol as an extension to AODV protocol. To apply authentication, each node has to verify the identity of another node before communicate with it. The authentication method performs without need for the trusted third- party this authentication revealed from the SRP authentication algorithm (Wu, 1998). The protocol does not require to modify the four control packets' structure (hello, route request, route reply and route error) that already in ADOV. Instead, it is added two new Packets (KeyExchange and Authentication packets) for the purpose to obtain shared secret key between two neighbor nodes and authentication. In the Key Exchange packet, a Diffie-Hellman algorithm applies to collect a shared key required as a password in the authentication process. The packet authentication exploits the shared secret found in Key exchange to exchange parameters between two neighbors' nodes. These parameters are used to verify the identity of each node involved in route discovery. This algorithm limited the using of the trusted party in authentication stage, which is difficult to be established. However, any node rejects cooperation and has a selfish behavior result in an incomplete authentication.

1.16. Unobservable Secure on-Demand Routing Protocol (UBSOR)

This protocol (Wan *et al*., 2012) achieves high privacy on reactive route by observed the packets' content in the network. Observed packet content means to hide the content of the control and data packet by encryption methods. In this protocol, each node has to acquire a group signing key and ID private key from a server when the first-time joints the network. The routing protocol based on this protocol includes two stages: anonymous key establishment and Route discovery. The first stage executes to construct two key sessions among nodes' neighbors without knowing each other. One key is the shared key used for route reply and packet forward and the second key is local broadcast key used for the route discovery. In route discovery, the source encrypts the source id, distention id and random number by the means can only open by the destination private key. Encrypted packet is broadcasted with a signature that can be verified by the node neighbors using key group. Each node has to verify the signature then continue to broadcast the encryption packet with their signature. Finally, the destination received and decrypts the packet and start route reply. In route reply each node used the

shared key to verify the packet reply. The protocol is difficult to attack since the packet is encrypted and only known the content by the destination. However, it needs third parties to establish of the key.

1.17. ADOV Security Extension (AODVSEC)

This protocol is secured ADOV from faked route reply only (Aggarwa *et al*., 2012). The Route Request is similar to the ADOV but has two new fields, the previous hope and the request time. However, there is a new control message named Route Request Acknowledgment (RREQ-ACK). RREQ-ACK is sent by each node desire to send route reply and not broadcast the route request. It also has a table called Rout REQest Acknowledgment (RREQ-ACK) cache contained information to validate any incoming reply packet. The table contains parameters, which are a source, a destination, a time stamp, a Boolean flag and expire time. Boolean flag requires indicating the route request message received it duplicate route request, or it is RREQ-ACK. In route reply the node received a reply message; it first has to check the information on the reply message match with information in the RREQ-ACK cache. If the verification corrects the reply process continues. Otherwise the reply will not process and will not continue. The algorithm is simple, but it still easy exposed so many types of attacks.

1.18. Secure Time Ordered routing Protocol (STOP)

STOP is a special protocol to secure on- demand routing based on time ordering (Dabideen and Garcia-Luna-Aceves, 2012). The protocol has three concepts, which are time-based ordering, performance-based path selection and feedback from the destination. The time ordering based is utilized to build Direct Acrylic Graph (DAG) to find a multiple path between source and destination consideration. In this stage, the node will assort its neighbor to successful or successor, predecessor, or neutral corresponding to the destination depending on the relative time when the node receives and sends the request. In path selection, the node route packets through successor nodes depend on their past performance. The performance is determined through destination feedback for the packets received. The destination has to send periodically reply to inform the path nodes of their performance. Still STOP needs a third party to build a signature key, which is used during the packet routing to authentication the original of the packet and previous node. However, STOP can handle from different types of the attack such as a wormhole attack.

1.19. Secure Efficient Distance Vector Routing (SEAD)

SEAD (Hu *et al*., 2003a; Hu and Perrig, 2004) is implemented as part of Destination-Sequenced Distance-Vector routing protocol (DSDV) that is considered as proactive topology (Charles *et al*., 1994). In SEAD the routing update will be secured through the authentication as well as the receiver authenticates the sender. One approach used for authentication is one-way hash chain function (Hu *et al*., 2003b) that does not need expensive operations since it is symmetric cryptography. The hash chain function applies to verify the metric and sequence number of routing update to be modified by an attacker. That is no malicious node can increase the sequence or decrease the metric for the current routing. To release routing update message from routing free that may be created by an attacker a mechanism can be used to authenticate the number such as TESLA (Perrig *et al*., 2000; 2001) or simpler one shared key.

1.20. Securing OLSR

Clausen *et al*. (2003) proposed security routing belongs to the proactive routing protocols and performs as an extension to Optimized Link-State Routing Protocol (OLSR) (Adjih *et al*., 2003). It is based on authentication check of the control messages and timestamps to evaluate the freshness of the messages. For authentication, each node generates a signature for the message to be omitted. The node that received the message must verify the receiving message to ensuring the originated of the message. Public key or shared key can be used for authentication. The timestamps are used to specify the freshness of the message if it is old or current to prevent replay attack.

1.21. Secure Multipoint Relay based Routing (SMRR)

The protocol (Saha *et al*., 2012) is secured proactive method based on OLSR. The trust scheme is involved to select a multiple point (nodes) as administrator. These admin nodes perform secure routing between nodes. The selection of administrative nodes depends on two factors. One is the willingness calculation. Willingness calculation value derived as a summation of battery power of the node the coverage area (number of nodes that distance one or two hops) and the reliability (the node position range). The second is the trust value which obtains during message transfer. The trust value updates by using acknowledgment packet. Furthermore, each message is sent with signature for authentication purpose. The admin nodes

are a subset of the network to create a fully connected network. The admin nodes are responsible for relaying packets in the network. This protocol comes in new idea to make the high trusted nodes as admin. On the other hand, it is difficult to build like this protocol in low density nodes.

1.22. Secure Forwarding Packet

Securing the forwarding packet protocols still have little attention. There are few studies that concentrated on this area. To secure packet forwarding the routes that are used for transmission the packet must also be secured. That mean forwarding protocols must be applied on one of the secured routing discovery protocols. If a single path is used to send a data packet, any malicious nodes along this path easy to endanger it. Even so, if the data is divided to a number of pieces and transfer through multiple disjoint paths. The malicious nodes require getting all the pieces to compromise the messages. The next describes protocols to secure data forwarding using multipath routs.

1.23. Secure Message Transmission (SMT) and Secure Single Path (SSP) Protocols

To secure the data transmission Secure Message Transmission (SMT) protocol or Secure Single Path (SSP) protocol could be used (Papadimitratos and Haas, 2003; Papadimitratos and Haas, 2006; Papadimitratos, 2005). In both protocols the packet to be transferred dispersed on the discovery route(s). This scheme is based on Rabin's algorithm (Rabin, 1989), which is considered, in essence, as a fault recovery code. By using this algorithm a limited redundancy is added to the data to allow recovery from a number of faults. The aim of SMT is to ensure secure data forwarding on different route paths, after the discovery of routes between the source and the destination has been performed. The source and destination use a set of diverse, node-disjoint paths that are considered valid for that time. These set of paths are named the Active Path Set (APS). SMT uses an APS to disperse for each outgoing message, adding limited redundancy to the data using and dividing the resultant information into pieces, which are transmitted across the APS routes one piece per route. For example, a packet is divided into four pieces using Rabin's algorithm as shown in **Fig. 5**. The source sends four pieces on independence multipath routes. If the destination receives three pieces, it can recover the packet without the need of the lost pieces.

SSP protocol utilizes a single route. SSP does not incur multi-path transmission overhead. SSP can be considered a limited case of SMT. SSP provides lower transmission overhead than SMT.

1.24. REliable and Efficient Forwarding (REEF)

REFF (Conti *et al*., 2006) is multi-path routing protocols that discovers multiple routes to a destination and selects the best route to forwarding the packet. REEF determines the forwarding misbehaving due to intentional actions, malicious and selfish nodes. REFF is based on reliability mechanism. The goal of this approach is to improve performance of forwarding message and balancing network utilization at the same time. The nodes in this mechanism are not only responsible for forwarding packet, but they also have to forward on the route with maximum reliability (high successful probability route). In order to find reliable routes, every node in REFF has a dynamic reliability updateable table that contains the reliability value to each outgoing link to a neighbor. Each time node sends a packet on a path to a neighbor node; an updating to the reliability value associated to neighbor node is occurred. If the packet delivery succeeded, then the updating is positive otherwise it is negative. Moreover, REEF can support secure node communication in the situation when there is a security association at the endpoints. The source and destination negotiate using shared key that will be used by destination to verify the Message Code Authentication (MAC) that carries in the message. In this way, the packets' transmission does not require any cryptographic operation at the intermediate nodes. REEF considered a lightweight aspect in terms of energy consumption as well as computational algorithms.

1.25. Security Protocol for Reliable Data Delivery (SPREAD)

SPREAD scheme (Lou *et al*., 2004) enhances the confidentiality and availability statistically by using multipath routing. The first step in this protocol is to find disjoint multipath routing by using one of the multipath routing algorithms. At the source, the message is divided to a number of pieces named shares using a Threshold Secret Sharing algorithm (Shamir, 1979; Simmons, 1995). The threshold Secret Sharing algorithm divides the message to N shares with redundancy, while the original messages can be rebuilt at the destination uses T (T<N) shares. Afterward, each shares decrypts with different key and transmits on different paths. Even the one attacker or more interrupt one path or more, it is required T shares to reconstruct the original message. Moreover, the decryption process is hard to recover since each share is encrypted with different keys. The SPREAD is capable of enhancing the confidentially and availability by encryption method and the threshold secret sharing algorithm.

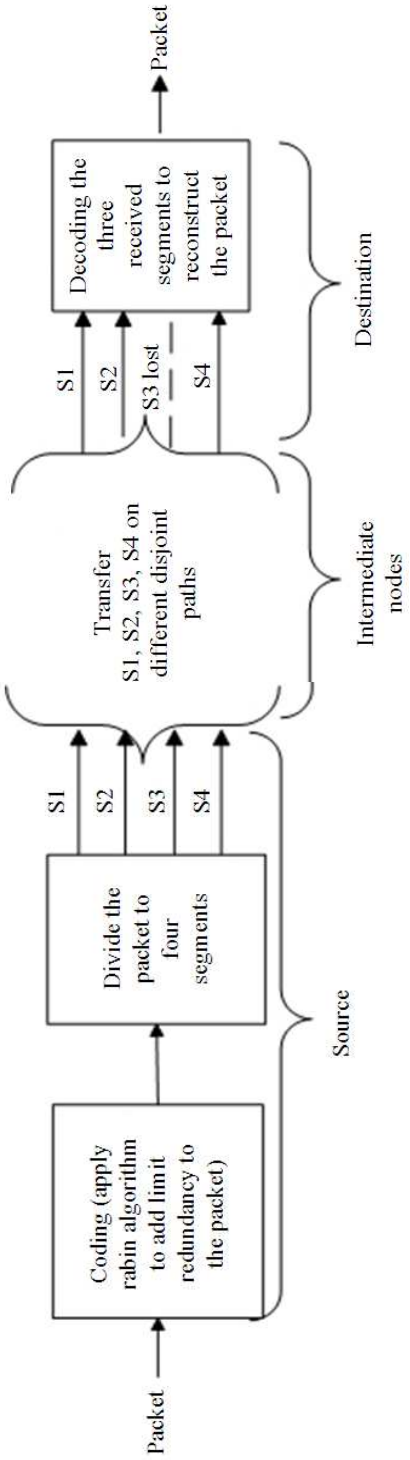

Fig. 5. Example of Secure Message Transmission (SMT): there are four disjoint paths, the packet is coding by Rabin's algorithm with redundancy factor = 4/3 where 3 is the min-imum number of segments need to reconstruct the packet

Table 1. Summary for secure routing protocols properties

Protocol Name	Routing topology	Security associative	Cryptography type	Security requirements	Advantage	Disadvantages	Rushing attack	Black hole attack	Wormhole attack	Jellyfish attack
SRP	Reactive	Ended nodes	Symmetric	Integrity, authentication	no overhead computation in intermediate nodes	Can be attacked with nodes colluding	No	No	Yes	Yes
Ariadne	Reactive	All nodes	Symmetric	Integrity, authentication	Immune to the wormhole attack	Based on time synchronization which is difficult to implement	No	No	Yes	Yes
TARP	Reactive	None	Both	Availability	Save resources	need to combine to one of the security protocols	Yes	Yes	Yes	Yes
SecMR	Reactive	All nodes	Asymmetric	Authentication	Secured multipath route	Overhead for computation in each intermediate nodes	No	No	Yes	Yes
SEDYMO	Reactive	None	Both	Authentication integration	Prevent attack of modified the hop counts and the non altered field	Overhead for computation in each intermediate nodes	No	No	Yes	Yes
SERA	Reactive	None	Both	Authentication and integration	Prevent modified attacks for hops number and sequence number	Require loosly synchronization, distribution for authentication vow	No	No	Yes	Yes
MOSAR	Reactive	None	Both	Authentication integration and no repudiation	Can balance between security performance and power consuming	The problem of security level classification	No	Yes	Yes	Yes
APPALLS	Reactive	All nodes	Both	Integrity, Authentication	Can isolate the misbehaving nodes	Can have problem of wormhole attack	No	No	Yes	Yes
ASRP	Reactive	All nodes	Both	Authentication and integration	Apply Strong Authentication	Cannot prevent from wormhole attack and selfish node can halt protocol	No	No	Yes	Yes
UBSOR	Reactive	Neighbor nodes	Both	Authentication and integration	strong privacy protection	Cannot handle worm hole attack	No	No	Yes	Yes
AODVSEC	Reactive	None	None	integration	No computation due to lack of cryptography	Cannot protect request packet	Yes	No	Yes	yes
STOP	Reactive	Ended nodes	Asymmetric	Authentication integration and no repudiation	Can select path depends on performance	Need key management and overhead for encrypt the packets	No	No	No	No
SEAD	Proactive	All nodes	Symmetric	Authentication	Attacker creating routing loops can be prevented	Does not cope with wormhole attacks	No	No	Yes	Yes
Secure OLSR	Proactive	All nodes	Both	Authentication	Prevent play attacks and modified the routing path	Vulnerable to wormhole attack	No	No	Yes	Yes
SMRR	Proactive	none	Asymmetric	Integrity and confidentiality	Depend on Trust nodes to relay the packets	Can not apply in low density network	No	No	Yes	No

1.26. Securing Data Based Multipath Routing in Ad Hoc Networks (SDMP)

Othman and Mokdad (2010) propose a new protocol, requires to find disjoint multi paths between source and destination. The first issue is to divide the original messages to a number of pieces named shares with unique identifier. These shares are combined using XOR operations then encrypt to impose confidentially. At least, three paths require to be discovered to transmit the shares. One path is used for signaling. To transmit number of shares and a random number that is specified one of the share identifiers. The second path transmits the plain text of share specified by random numbers and shared key. The other link is used to transmit the other combined pairs. If there is a path failure, the data can be recovered using Diversity Coding method (Ayanglou *et al*., 1993). The potentiality of the attacker can construct the message is very low since it is required to get all the shares.

1.27. Context Free Protocol

This protocol is proposed to remove the effect of the selfish nodes (Aggarwa *et al*., 2012). The basic solution to selfish nodes is detected the misbehaving nodes then either prevent them or punish them. However, the context free protocol does not depend on this solution.

Instead, it enforces the selfish node to cooperate by hiding the identity of the destination and packet details. The identity of the destination can be known from the last hop along the route path and from data packet. The information about destination and route path will be removed from data packet. Since the route, path is removed, the data packet is forwarding by broadcasting it with some type of route loop. This loop is required to mock the selfish nodes that it may be a destination for this packet. Therefore, the selfish node should participate in the packet relays since it does not know if the packet sent to it or not. Each node in this protocol has to generate public key and private key during joint network. The source encrypts the data packet with public key of each node maintains the route request but in reverse order. A hash key is used by each node to determine whether it is destination, or it is part of the route path. The packet is dropped when the node is neither a destination nor on the route path. The selfish node should participate in the packet relays since it does not know if the packet sends to it or not.

2. CONCLUSION

The area of ad hoc network security has been receiving increase interest in the recent years. The security of Mobile Ad Hoc Network is very difficult issues due to lack of central management. In this review, we attempt to explain the protocols protected route discovery from malicious nodes in both reactive and proactive topologies. All the protocols for security route discovery used cryptographic methods to perform the security with establishment of associative security. To secure data communications, we have to apply secure routing discovery first to ensure the validity of the used routing path. The protocol performance has to make balance between security power and source limitations. For the data communication security, redundancy requires to obtain availability requirement. For future works, we can attempt to apply these protocols to hybrid topology that they need some modification so that can be suited to these topologies. In addition, all these protocols are securing the data or routes' path without an attempt to prevent the paths from malicious nodes. **Table 1** gives a summary review to some properties of securing routing protocols, advantages and disadvantages as well as the different types of attacks can be handled.

3. ACKNOWLEDGEMENT

This research work is supported by the Research University Grant Scheme (RUGS), Universiti Putra Malaysia (RUGS Number: 05/03/10/1039RU).

4. REFERENCES

Abusalah, L., A. Khokhar and M. Guizani, 2006. Trust aware routing in mobile ad hoc networks. Proceedings of the IEEE Global Telecommunications Conference, Nov. 27-Dec. 1, IEEE Xplore Press, San Francisco, CA., pp: 1-5. DOI: 10.1109/GLOCOM.2006.264

Adjih, C., T. Clausen, A. Laouiti, P. Mühlethalerand and D. Raffo, 2003. Securing the OLSR protocol. Proceedings of the 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop, (IAMAHNW' 03), Mahdia, pp: 25-35.

Aggarwa, A., S. Gandhi, N. Chaubey, P. Shah and M. Sadhwani, 2012. AODVSEC: A novel approach to secure Ad Hoc on-Demand Distance Vector (AODV) routing protocol from insider attacks in MANETs. Int. J. Comput. Networks Commun., 4: 191-210. DOI: 10.5121/ijcnc.2012.4412

Al-Shurman, M., S. Yoo and S. Park, 2004. Black hole attack in mobile ad hoc networks. Proceedings of the 42nd Annual Southeast Regional Conference, Apr. 02-03, ACM Press, New York, USA., pp: 96-97. DOI: 10.1145/986537.986560

Anjum, F. and P. Mouchataris, 2007. Security for Wireless ad hoc Networks. 1st Edn., John Wiley and Sons, Hoboken, ISBN-10: 0470118466, pp: 316.

Ayanglou, E., I. Chil-Lin, R. Gitlin and J. Mazo, 1993. Diversity coding for transparent self-healing and fault-tolerant communication networks. IEEE Trans. Commun., 41: 1677-1686. DOI: 10.1109/26.241748

Chakeres, I. and C. Perkins, 2007. Dynamic MANET On-demand Routing Protocol. University of California Santa Barbara.

Charles, E., A. Perkins and P. Bhagwat, 1994. Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers. Proceedings of the Conference on Communications Architectures, Protocols and Applications, Aug. 31-Sep. 02, ACM Press, New York, USA., pp: 234-244. DOI: 10.1145/190314.190336

Clausen, T., P. Jacquet, C. Adjih, A. Laouiti and P. Minet *et al*., 2003. Optimized Link State Routing Protocol (OLSR). Network Working Group.

Conti, M., E. Gregori and G. Maselli, 2006. Reliable and efficient forwarding in ad hoc networks. Ad Hoc Netw., 4: 398-415. DOI: 10.1016/j.adhoc.2004.10.006

Dabideen, S. and J. Garcia-Luna-Aceves, 2012. Secure routing in MANETs using local times. Wireless Netw., 18: 811-826. DOI: 10.1007/s11276-012-0435-2

Deng, H., W. Li and D. Agrawal, 2002. Routing security in wireless ad hoc networks. IEEE Commun., 40: 70-75. DOI: 10.1109/MCOM.2002.1039859

Helena, R. and H. Jordi, 2007. Secure Dynamic MANET On-demand (SEDYMO) routing protocol. Proceedings of the 5th Annual Conference on Communication Networks and Services Research, May 14-17, IEEE Xplore Press, pp: 372-380. DOI: 10.1109/CNSR.2007.57

Hongwei, L. and P. Atam, 2010. MOSAR: A secure on-demand routing protocol for mobile multilevel ad hoc networks. Int. J. Netw. Security, 10: 121-131.

Hu, Y., A. Perrig and D. Johnson, 2003d. Packet leashes: A defense against wormhole attacks in wireless networks. Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications, Mar. 30-Apr. 3, IEEE Xplore Press, pp: 1976-1986. DOI: 10.1109/INFCOM.2003.1209219

Hu, Y.C. and A. Perrig, 2004. A survey of secure wireless ad hoc routing. IEEE Security Privacy, 2: 28-39. DOI: 10.1109/MSP.2004.1

Hu, Y.C., A. Perrig and D.B. Johnson, 2003b. Efficient security mechanisms for routing protocols. Proceedings of the 10th Annual Network and Distributed System Security Symposium, (NDSS' 03), pp: 57-73.

Hu, Y.C., A. Perrig and D.B. Johnson, 2003c. Rushing attacks and defense in wireless ad hoc network routing protocols. Proceedings of the 2nd ACM Workshop on Wireless Security, Sep. 19-19, ACM Press, New York, USA., pp: 30-40. DOI: 10.1145/941311.941317

Hu, Y.C., A. Perrig and D.B. Johnson, 2005. Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless Netw., 11: 21-38. DOI: 10.1007/s11276-004-4744-y

Hu, Y.C., D.B. Johnson and A. Perrig, 2003a. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Netw., 1: 175-192. DOI: 10.1016/S1570-8705(03)00019-2

Imad, A., J. Hubaux and E. Knightly, 2004. Denial of service resilience in ad hoc networks. Proceedings of the 10th Annual International Conference on Mobile Computing and Networking, Sep. 26-Oct. 01, ACM Press, New York, USA., pp: 202-215. DOI: 10.1145/1023720.1023741

Komninos, N., D. Vergados and C. Douligeris, 2007. Detecting unauthorized and compromised nodes in mobile ad hoc networks. Ad Hoc Netw., 5: 289-298. DOI: 10.1016/j.adhoc.2005.11.005

Kulasekaran, S. and M. Ramkumar, 2011. APALLS: A Secure MANET Routing Protocol. In: Mobile Ad-Hoc Networks: Applications, Wang, X. (Ed.), InTech, ISBN-10: 9789533074160.

Li, Q., Z.Y. Hu, M. Zhao, A. Perrig and J. Walker *et al*., 2008. SEAR: A secure efficient ad hoc on demand routing protocol for wireless networks. Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, Mar. 19-20, ACM Press, Tokyo, Japan, pp: 201-204. DOI: 10.1145/1368310.1368339

Lou, W., W. Liu and Y. Fang, 2004. SPREAD: Enhancing data confidentiality in mobile ad hoc networks. Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications, Mar. 7-11, IEEE Xplore Press, pp: 2404-2413. DOI: 10.1109/INFCOM.2004.1354662

Maheshwari, R., 2007. Detecting wormhole attacks in wireless networks using connectivity information. Proceedings of the 26th IEEE International Conference on Computer Communication, May 6-12, IEEE Xplore Press, Anchorage, AK., pp: 107-115. DOI: 10.1109/INFCOM.2007.21

Mavropodi, R., P. Kotzanikolaou and C. Douligeris, 2006. SecMR-a secure multipath routing protocol for ad hoc networks. Ad Hoc Netw., 5: 87-99. DOI: 10.1016/j.adhoc.2006.05.020

Nabet, A., R. Khatoun, L. Khoukhi, J. Dromard and D. Gaiti, 2011. Towards secure route discovery protocol in MANET. Proceedings of the Global Information Infrastructure Symposium (GIIS), Aug. 4-6, Da Nang, pp: 1-8. DOI: 10.1109/GIIS.2011.6026717

Othman, J. and L. Mokdad, 2010. Enhancing data security in ad hoc networks based on multipath routing. Parall. Distribut. Comput., 70: 309-316. DOI: 10.1016/j.jpdc.2009.02.010

Papadimitratos, P. and Z. Haas, 2002. Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), Jan. 27-31, IEEE San Antonio, TX., pp: 193-204.

Papadimitratos, P. and Z. Haas, 2003. Secure message transmission in mobile ad hoc networks. Ad Hoc Netw., 1: 193-209. DOI: 10.1016/S1570-8705(03)00018-0

Papadimitratos, P. and Z. Haas, 2006. Secure data communication in mobile ad hoc networks. IEEE J. Selected Areas Commun., 24: 343-356. DOI: 10.1109/JSAC.2005.861392

Papadimitratos, P., 2005. Secure and fault-tolerant communication in mobile ad hoc networks. Ph.D. Dissertation, Cornell University, Ithaca, New York.

Papadimitratos, P., Z. Haas and P. Samar, 2002. The Secure Routing Protocol (SRP) for Ad Hoc Networks. IETF Internet, Draft RFC 2026.

Perrig, A., R. Canetti, D. Song and D. Tygar, 2000. Efficient authentication and signing of multicast streams over lossy channels. Proceedings of the IEEE Symposium on Security and Privacy, (ISSP' 00), IEEE Xplore Press, Berkeley, CA., pp: 56-73. DOI: 10.1109/SECPRI.2000.848446

Perrig, A., R. Canetti, D. Song and J.D. Tygar, 2001. Efficient and secure source authentication for multicast. Proceedings of the Network and Distributed System Security Symposium (NDSS'01), CiteSeerX, pp: 35-46.

Rabin, M., 1989. Efficient dispersal of information for security, load balancing and fault tolerance. J. ACM, 36: 335-348. DOI: 10.1145/62044.62050

Ramaswamy, S., H. Fu, M. Sreekantaradhya, J. Dixon and K. Nygard, 2003. Prevention of cooperative black hole attack in wireless ad hoc network. Proceedings of the International Conference on Wireless Networks, (ICWN' 03), CiteSeerX.

Saha, H., D. Bhattacharyya and P.K. Banerjee, 2012. Secure multipoint relay based routing in MANET. Proceedings of the 2nd International Conference on Computational Science, Engineering and Information Technology, Oct. 26-28, ACM Press, New York, USA., pp: 63-68. DOI: 10.1145/2393216.2393228

Sanzgiri, K., B. Dahill, B. Neil, B. Levine and C. Shields *et al*., 2002. A secure routing protocol for ad hoc networks. Proceedings 10th IEEE International Conference Network Protocols, Nov. 12-15, IEEE Xplore Press, pp: 78-87. DOI: 10.1109/ICNP.2002.1181388

Shamir, A., 1979. How to share a secret. Commun. ACM, 22: 612-613. DOI: 10.1145/359168.359176

Simmons, L.W., 1995. Relative parental expenditure, potential reproductive rates, and the control of sexual selection in katydids. Am. Naturalist, 145: 797-808.

Sivakumar, K. and M. Ramkumar, 2008. Improving the resiliency of Ariadne. Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks, IEEE Xplore Press, Newport Beach, CA., pp: 1-6. DOI: 10.1109/WOWMOM.2008.4594927

Tamilselvan, L. and V. Sankaranarayanan, 2006. Solution to prevent rushing attack in wireless mobile ad hoc networks. Proceedings of the International Symposium on Ad Hoc and Ubiquitous Computing, Dec. 20-23, IEEE Xplore Press, Surathkal, pp: 42-47. DOI: 10.1109/ISAHUC.2006.4290645

Wan, Z., K. Ren and M. Gu, 2012. USOR: An unobservable secure on-demand routing protocol for mobile ad hoc networks. IEEE Trans. Wireless Commun., 11: 1922-1932. DOI: 10.1109/TWC.2012.030512.111562

Wu, T., 1998. The secure remote password protocol. Proceedings of the Internet Society Network and Distributed System Security Symposium, (ISNDSSS' 98), CiteSeerX, pp: 97-111.