ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 10, October 2015

Analysis of Security Issues, Challenges and Current Trends in AODV and DSR

Harsha Sharma

Dept of Computer Engineering, YMCA University of Science and Technology, Faridabad, Haryana, India

Abstract: Mobile ad hoc networks (MANET) have garnered considerable research interest owing its popularity to the significant advantages it offers over traditional wireless networks. Recent research in ad hoc networks has focused on implementing secure routing protocols. However singular characteristics of MANET topology namely peer-to-peer architecture, lack of centralized management, resource constraints (battery, bandwidth and computation capacity) and dynamic topology pose significant challenges to security solutions.
In this paper, we detail security threats and limitations of AODV [1] and DSR [2] Routing Protocol. We identify the current secure protocols based on AODV and DSR – SAODV, SAR, ARIADNE, SRP and ARAN. We examine the advantages and disadvantages of each secure protocol and compare them based on certain security parameters.

Keywords: MANET, AODV, DSR, SAODV, SRP, ARIADANE, ARAN, TAODV, SRP.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile nodes that form a network by routing messages for each other without a fixed infrastructure. Nodes depend on each other for performing networking functions such as packet forwarding, routing and service discovery. Ad-hoc networks are inherently infrastructure less and are thereby cost effective. These characteristics make ad hoc networks efficient in situations where setting up an infrastructure is not possible or we do not have the financial support for the same. Ad hoc networks are utilized in the following fields: military, sensor networks, disaster area network and personal area network.

Routing Protocols can be divided into three broad categories: Proactive, Reactive and Hybrid Protocols. Proactive protocols are also known as table-driven routing protocols. Each node maintains information about every other node in the network topology. Reactive Protocols are also known as on-demand routing protocols. Nodes use a query – reply system to know the path to a destination only when the need arises. Hybrid protocols utilize both proactive and reactive approaches. They switch between these two approaches.

We detail the exploits and vulnerabilities of two on – demand protocols: Ad hoc On-Demand Distance Vector (AODV) [1] and Dynamic Source Routing (DSR)[2] on account of their dynamic nature, better performance with lesser overhead and wide acceptance. AODV and DSR were designed to work efficiently in a ubiquitous scenario that is devoid of any malicious nodes. All the nodes were assumed to be trustworthy and credible. But, this not the case in realistic networks (hostile environment) where the loopholes in the algorithm of these protocols can be exploited.

This paper is organized as follows: Section II gives a brief description of the functionality of AODV and DSR routing protocols. Section IIIillustrates the vulnerabilities common to AODV and DSR on account of on-demand routing protocols.Furthermore, we analyse the exploits specific to both the protocols. Section IV presents the limitations posed by AODV and DSR. Section V discusses the current secure routing protocols based on AODV and DSR. We also present tabular analyses on the secure routing protocols.

II. PROTOCOL OVERVIEW

AODV Routing Protocol Overview

AODV (Ad Hoc On-Demand Distance Vector) Routing [1] is a reactive routing protocol i.e. AODV initiates route discovery only when such a requirement arises. Nodes in a network topology implementing AODV Routing Protocol do not maintain routes to every other node in the network. Whenever a node needs to send a packet it checks its routing table to determine whether it has a current route to the destination. If a current route is found then the packet is unicasted to the destination but if no current route is found a route discovery process is initiated. Route Discovery process begins with the creation of a Route Request Packet (RREQ) by the source node. RREQ contains the following fields: Broadcast ID, source node's IP address, source node's current sequence number, destination IP address and destination sequence number. Broadcast ID gets incremented each time a source initiates a route discovery process through RREQ. The destination sequence number in the RREQ is the most recent sequence number for the destination of which the source is aware. RREQ is broadcasted via flooding. When an intermediate node receives an RREQ packet it makes a Reverse Route entry for the source node in its routing table. Reverse route contains the following fields: source IP Address, source sequence number, number of hops to the source node and IP Address of the node from which RREQ was received. A node may send a route reply (RREP) to the source if it is the destination node or if it contains a route to the destination with a sequence number greater or equal to the destination sequence number in the RREQ. The node use the combination of Broadcast ID and source sequence number to uniquely identify the RREQ and thereby discard the RREQ if they receive it again from some other

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 10, October 2015

intermediate node. Once the RREP is received by the source node it can start transmitting the data packets to the destination.

DSR Routing Protocol Overview

DSR [2] is a reactive protocol for mobile ad hoc networks and is similar to AODV [1] as it queries the network through RREQ packet whenever the requirement for a route arises. Though it shares the features of on-demand routing with AODV but its employs source routing and route caching, features which make it fundamentally different from AODV routing protocol.

TABLE I COMPARISON OF AODV AND DSR

Property	AODV	DSR
Routing Philosophy	Hop by hop	Source Routing
Multicast Capability	Yes	No
Multiple Routes	No	Yes
Routes maintained in	Route table	Route cache
Timers for expiry	Yes	No
Routing metric	Freshest and shortest path	Freshest path
Possibility of unidirectional link support	No	Yes
Route Reconfiguration Strategy	Erase route then source notification	Erase route then source notification or local route repair

Each node adds its own identifier to the route record and forwards the RREQ to the next node. This feature is known as source routing as the entire route from the source to the destination is recorded in the RREQ. An intermediate node discards the RREQ if it has the same Request ID i.e. the RREQ has already been forwarded by the node before. When the RREQ reaches the destination node, the destination node copies the route is RREQ into the RREP and replies to the source. Sender upon receiving the RREQ caches the route in its route cache for subsequent routing. Unlike AODV, DSR allows the intermediate nodes to cache multiple routes to one destination in its route cache. Also, a node can learn about the neighbouring routes by promiscuous listening.

Each RREQ packet contains a field called hop limit. Hop limit, set by the source, is used to specify the number of permissible intermediate nodes between the source and the destination. Every intermediate node decrements the hop limit by 1 before forwarding the RREQ to its neighbouring node. The RREQ is discarded, even if it has not reached the destination node, if the hop limit becomes zero. Table I [3] illustrates the differences between AODV and DSR.

III. VULNERABILITIES IN AODV AND DSR

AODV and DSR are similar on the basic level as both are on-demand routing protocols. Consequently certain vulnerabilities affect both the ad hoc routing protocols but other attacks are specific, exploiting the loopholes in the algorithm governing the protocol.

In the next section we illustrate the attacks common to both protocols.

A. Attacks Common to AODV and DSR

i)Wormhole Attack or Tunnelling :

[4][5] In this type of attack a 'tunnel' is created between two malicious nodes which directly links these two nodes by bypassing all other nodes in the path. This prevents the discovery of authentic paths to the destination since the two colluding nodes advertise that they are one hop count apart and hence have the shortest path to each other. If the tunnel is used honestly then the network is not compromised and rather efficiency of the network increases but if the attacker chooses to use the tunnel to its advantage then significant harm can be done.

The numbers of ways two colluding nodes can compromise the network through a 'wormhole' are:

- **Denial-of-Service** : The attacker can discard all the packets intended for the destination node and thereby create a permanent denial-of service attack
- **Selectively discard** the data packets similar to the technique employed in gray hole attack.
- **Modification of data packets**
- **Passive attack** such as eavesdropping which compromises the message integrity

ii)Sender or Recipient Anonymity Attack

In both AODV and DSR Routing Protocol the RREQ packet employed for querying the network topology is embedded with the source and destination address. A malicious node which has intercepted such a flooded packet can uniquely identify the sender's and recipient's identity, though it might not be able to decipher the vertex/location of the sender and recipient nodes.

iii) Impersonation or Spoofing

RREQ packet used by AODV and DSR to query the network contain Source Address and Destination Address fields. These fields can be easily spoofed using publicly accessible tools. Through spoofing an attacker can alter the network topology or isolate a node from the network.

iv) Traffic Analysis Attack

Using Traffic Inference algorithm [6], an adversary can decode the MANET traffic pattern. The algorithm assumed the relation between data frames, routing frames, and MAC frames enable to the passive observer, which permits the observers to detect the single-hop traffic using MAC frames, thereby allows to find the multi-hop traffic using routing frames and finally traces the traffic pattern using data frame. The simulation result shows TIA can infer the traffic pattern with an accuracy of nearly 95%.

v) Rushing Attack

Rushing attacks exploit the route discovery process. AODV and DSR use duplicate suppression during the route discovery and are therefore vulnerable to this attack. When a compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet can react. So when the nodes receive the original RREQ from source, they simply discard it. In this case, source fails to discover any

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 10, October 2015

useable route or safe route without the involvement of attacker.

B. Security Issues in AODV

i) Incrementing the Sequence Number (Black hole and Gray hole Attack):

A malicious node replies with a RREP packet with a modified incremented sequence number when it receives an RREQ. So, the source node ignores other routes as it assumes that the malicious node has the freshest route to the destination and begins transmitting the data packets over the malicious node. Consequently, the malicious node gains unrestricted access to the data packets and it discards all the data packets intended for the destination node. This attack is known as black hole attack because like a 'black hole' it 'swallows' all the data packets [6]. In gray hole attack, instead of discarding all the data packets, which is the case with black hole attack, the malicious node discards random packets. So, the malicious node's behaviour fluctuates between a normal node and compromised node. Gray hole attack is more difficult to detect as compared to black hole attack because of the selective forwarding behaviour displayed malicious node.

ii) Decrementing the hop count

AODV gives preference to higher sequence number as opposed to lower hop count but if the sequence number is same the route with lower hop count is chosen. In other words, AODV protocol chooses the shorter path if the route freshness (indicated by the sequence number) is same. A malicious node can exploit this characteristic of AODV protocol to advertise shorter route to the destination node and thereby redirecting all the data packets through itself. In this case, it gains access to all the data packets and can choose to do discard them or do anything else.

C. Security Issues in DSR

i) Altering the Source Route in RREQ

DSR uses source routing which entails explicitly stating routes in data packets. Nodes use promiscuous listening to add or modify their routing table entries. An adversary can modify the source routes in the data packets which will further result in addition, deletion or injection of false entries in the routing tables of other nodes. This vulnerability can be exploited by an attacker to poison the route caches to a node. Routing table poisoning attacks can result in selection of non-optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network.

IV. LIMITATIONS

AODV and DSR are on-demand routing protocols and consequently resource conserving (battery consumption and bandwidth) since they don't require periodic transmission of network topological information. This strategy is very efficient when the data transmission is sporadic and the volume and frequency of transmission is uncertain. In this section we analyse the limitations plaguing these two protocols. Section IV analyses the limitations common to AODV and DSR and those specific to each protocol.

A.Limitations of AODV and DSR Routing Protocol

- **Route setup latency**: The nodes query the network topology only when need arises. So, even if the data packets are ready for transmission, they are queued and forced to wait until a valid route to the destination is found through the route discovery process.
- **Route Reply Storms**: The intermediate nodes compare the destination sequence number mentioned in the RREQ packet with the sequence number, for the particular destination, available with them. If the sequence number available with them is higher than the one in RREQ, they reply with a corresponding RREP packet to the source. This technique can result in heavy control overhead and bandwidth consumption if the destination sequence number available with the source is very old and many intermediate nodes have higher but stale sequence number for that particular destination. In this case, the source receives multiple but useless RREPs.
- **RREP Collision:** If multiple intermediate nodes reply to the RREQ at the same time packet collision can occur at the source node which would result in the failure of the whole route discovery process. To avoid this situation, random delays in replying with RREP back to the source node can be used.

B. Limitations of AODV

AODV is a single-path protocol i.e. it maintains only a single route to a destination. The decision of optimal route selection is based upon the metrics of route freshness (sequence number) and length of the route (hop count). In this section we analyse the limitations posed by the AODV protocol:

- AODV uses sequence numbers to determine the freshness of a route between two nodes. Higher sequence number is the deciding factor which determines the acceptance of one route over another. It is a single path protocol: one and only one route to a destination is maintained based on a higher sequence number. This leads to the rejection of a valid route if it has a lower sequence number.
- An RREQ packet only learns a valid route to the destination and doesn't collect any data regarding the intermediate nodes in the network. In other words, it doesn't rely on source routing or promiscuous listening. So, we have to initiate a fresh RREQ even if the next destination node is located en route to the previous destination node.
- In AODV a node maintains only route to a destination and it has to invoke route discovery process if that route is rendered invalid. In a network topology with highly dynamic nodes this technique proves to be inefficient. Frequent initiation of route discovery leads to flooding of the network with RREQ packets which results in network congestion.

D. Limitations of DSR

The algorithm implemented by DSR was briefly described in Section II. Route caching and source routing though definitely beneficial, but also limit the algorithm is numerous ways. We analyse the limitations of DSR in this section:

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 10, October 2015

- Route Caching is employed by DSR to avoid initiating a route discovery every time data transmission is required. This technique significantly reduces network and congestion and negates route setup latency by obviating RREQ broadcasting. But in a highly dynamic network topology this strategy can be detrimental as the source node will try transmitting the data packets over numerous stale route entries in its cache before initiating a route discovery process.
- If an intermediate node replies with a stale entry from its route cache, it results in the pollution of the neighbouring nodes since they too add a stale entry in their route cache.
- Source Routing means that the RREQ packet header contains the entire route between the source and destination node. If the route between the source and the destination involves too many intermediate nodes it causes the packet header size to increase significantly.

V. CURRENT SECURITY TECHNIQUES FOR AODV AND DSR

A. SAODV (Secure Ad hoc On-Demand Distance Vector)

SAODV [7] is an improved version of the AODV routing protocol that addresses security concerns namely integrity, authentication and non-repudiation. SAODV enhances route discovery process, which provides many avenues to an intruder and overcomes vulnerabilities of traditional AODV. SAODV embeds popular techniques of network security in the transmission of RREQ: digital signatures and hash chains. The RREQ is bifurcated into two parts: mutable and immutable. Digital signatures are used to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). This is because for the non-mutable information, authentication can be performed in a point-to-point manner, but the same kind of techniques cannot be applied to the mutable information.

When an intermediate node receives a RREQ message, it first verifies the digital signature. Only if the digital signature is verified it follows the traditional mechanism of AODV. An intermediate node can reply with an RREP if it has a fresh route to the destination (determined by the sequence number). Since the intermediate node will have to digitally sign the RREP message as if it came from the destination, it uses the double signature extension described in this protocol. The only mutable field in RREP (hop count) is protected by hashing.

Vulnerabilities of AODV overcome by SAODV

- Modification of Destination and Source Address (Impersonation)
- Incrementing of hop count to advertise shortest route
- Incrementing Sequence number (Black hole and gray hole attack)

B. SAR (Security Aware Ad Hoc Routing)

SAR [8] uses trust levels to find a secure path for data transmission. SAR ensures that an intermediate node can only process the packet or forward it if the node itself can provide the required security or has the required authorization or trust level. The different trust levels are implemented using shared symmetric keys. In order for a node to forward or receive a packet it first has to decrypt it and therefore it needs the required key. If the node doesn't have the required key, the RREQ is dropped. Table II accurately describes the various security concerns and the measures implemented by SAR to tackle them.

TABLEIII TECHNIQUES EMPLOYED BY SAR

Property	Technique
Timeliness	Timestamp
Ordering	Sequence Number
Authenticity	Password, Security
Authorization	Credential
Integrity	Digest, Digital Signature
Confidentiality	Encryption
Non-repudiation	Chaining of digital signatures

If an end to end path with the required security attributes can be found, a suitably modified RREP is sent from an intermediate node or the eventual destination. The operation of SAR addresses the security of both routing and data exchange. SAR ensures a secure path from the source to the destination but it might not be the shortest route.

C. SRP (Secure Routing Protocol)

Secure Routing Protocol [9] provides a mechanism which can be applied to a multitude of reactive routing protocol. It protects against attacks that disrupt route discovery process and guarantees acquisition of correct topological information. Security Association (SA) is used between the source and destination which can verify the trusted node using shared secret key. It incorporates the security features into the forwarding mechanism. In the case of DSR [2] SRP requires a six word header containing unique identifiers that tag the route discovery process and message authentication code (MAC) computed using a keyed hash algorithm. An intermediate node measures the frequency of received queries from the neighbours. They provide a priority ranking as inversely proportional to the query rate. A malicious node will be given a low priority rank which results in it being served last or being ignored completely. The destination node verifies the integrity and authenticity of the received RREQ by computing the keyed hash of the request fields and comparing it with the MAC mentioned in the SRP header. If the RREQ is valid the destination node initiates a route reply (RREP) in the manner similar to the source. The source verifies the RREPs by matching the pending query identifiers and checks the integrity using the MAC generated by the destination. The route replies contain accurate and secure route to the destination which safeguards the network functionality. Similarly, route error messages can only be generated by nodes that lie on the route that is reported as

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 10, October 2015

broken. In order to guarantee this functionality, SRP determines explicitly the interaction with the network layer; i.e., the IP-related functionality. Since SRP requires a security association only between communicating nodes, it uses extremely light-weight mechanisms to prevent other attacks. For example, to limit flooding, nodes record the rate at which each neighbour forwards RREQs and gives priority to neighbours that less frequently forward the RREQs. Such mechanisms can secure a protocol when few attackers are present, however, such techniques provide secondary attacks such as sending fabricated RREQs to reduce the effectiveness of a node's authentic RREQs [12].

D. ARAN (Authenticated Routing for Ad-hoc network)

ARAN [10] provides authentication, message integrity and non-repudiation in ad-hoc networks by using a preliminary certification process which is followed by a route instantiation process that ensures end-to-end security services. But it needs the use of trusted certification server (T). A new node has to follow the following procedure before gaining entry in a network implementing ARAN Protocol:

- Request a certificate signed by T.
- The certificate is granted. It contains the IP address of the node, its public key, a timestamp of when the certificate was created and a time at which the certificate expires along with the signature by T.
- Join the network topology

All nodes are supposed to maintain fresh certificates with the trusted server and must know T's public key. ARAN defends a network against spoofing, fabrication and impersonation. But, it is susceptible to selfish nodes. A certified selfish node can cause significant harm to the network and ARAN does not propose any method to deal with such nodes. Also, ARAN is based upon asymmetric coding and electronic signature and hence it is vulnerable to attacks such as denial-of-service attacks. Furthermore, asymmetric coding is complicated and time consuming.

E. ARIADNE

Ariadne [11] relies on symmetric cryptography to ensure secure routing. It is based on the basic operation of DSR (Dynamic Source Routing). It can authenticate routing messages using one of three schemes:

- shared secret keys between all pairs of nodes
- shared secret keys between communicating nodes combined with broadcast authentication
- Digital signatures.

Source node sends an RREQ which contains: source address, destination address, an identifier that identifies the current route discovery, a TESLA time interval (represents the expected arrival time) and a hash chain. The intermediate node verifies the validity of TESLA time interval upon receiving the RREQ packet. Per-hop hashing technique is used to ensure authentication and integrity of RREQ which utilizes a one-way hash function. The source initializes the hash chain to a MAC with a key shared between the source and target. If the data packet is valid an intermediate node appends its own address in the node list, replaces the hash chain with a new one consisting of its address plus the old one and appends the MAC of the entire packet to the MAC list. The destination node validates each intermediate node by comparing the received hash with the computed hash of the MAC. ARIADNE provides as strong defence against modification and fabrication attacks. When it is used with an advanced version of TESLA known as TIK it provides security against wormhole attack. However, it is still vulnerable to selfish nodes. Ariadne is vulnerable to an attacker that happens to be along the discovered route. The node can't determine whether intermediate nodes are in fact forwarding packets that they have been requested to forward. So, there is no feedback (past history) of how the intermediate nodes are behaving [12].

F. TAODV

TAODV (Trusted AODV) [13] extends AODV [1] routing protocol and employs the idea of a trust model to protect routing behaviours in the network layer of MANETs. In the TAODV, trust among nodes is represented by opinion that is computed on the basis of three elements namely belief, disbelief and uncertainty. Routing Operations in TAODV can be divided into six steps:

i) Trust Recommendation: There are three types of messages: Trust Request Message (TREQ), Trust Reply Message (TREP), and Trust Warning Message (TWARN). Nodes who issue TREQ messages are called Requestor. Those who reply TREP messages are called Recommender. The recommendation target nodes are called Recommended.

ii) Trust Judgement: A node judges the trustworthiness by using the criteria described in Fig. 1.

belief	disbelief	uncertainty	Actions
		> 0.5	Request and verify digital signature
	> 0.5		Distrust a node for an expire time
> 0.5			Trust a node and continue routing
≤ 0.5	≤ 0.5	≤ 0.5	Request and verify digital signature

Fig.1. Criteria for Judging Trustworthiness

iii) Route Table Extension: Three new fields are added into each node's original routing table: positive events, negative events and opinion. Positive events are the successful communication times between two nodes. Similarly negative events are the failed communication ones. Opinion means this node's belief towards another node's trustworthiness as defined before.

DestinationIP	DestinationSeq	⋯	HopCount	⋯	Lifetime	Positive Events	Negative Events	Opinion

Fig.2. TAODV Routing Table

d) Trust Update: Trust Opinions are dynamic in nature and are subject to failed and successful communication between nodes. The trust updates are made in the following cases (1) Each time a node has performed a successful communication with another node (2) Each time a node has performed a failed communication with another node (3) Each time when the field of the successful or failed events changes, the corresponding

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 10, October 2015

value of opinion will be recalculated (4) If node's route entry has been deleted from node's route table because of expiry, or there is no route entry from the beginning.

e) Routing Messages Extensions: The message structure of TAODV adds the few fields in the original AODV message structure. Fig. 3 describes the Routing Message structure of TAODV.

f) Trusted Routing Discovery: Nodes use the employ described characteristics to find the route to the destination node. Opinions are the central metric used during routing discovery.

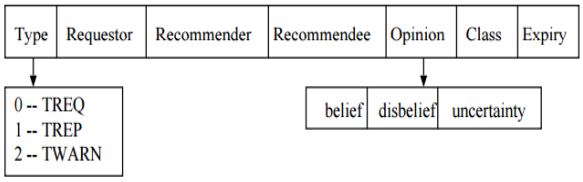

Fig. 3.Routing Message Structure

Table III summarizes the important differences between the security protocols discussed in Section V.

TABLE III **COMPARISON OF SECURE ROUTING PROTOCOLS**

Protocol	**ARAN**	**ARIADNE**	**SAODV**	**SRP**	**TAODV**	**SAR**
Type	Reactive	Reactive	Reactive	Reactive	Reactive	Reactive
MANET Protocol	AODV/DSR	DSR	AODV	DSR/ZRP	AODV	AODV
Central Trust Authority	Certificate Authority(CA) needed	Key Distribution Center(KDC) needed	Certificate Authority(CA) needed	Certificate Authority(CA) needed	Not Required	Not Required
Synchronization	No	Yes	No	No	No	No
Encryption Algorithm	Asymmetric	Symmetric	Symmetric	Symmetric	Not Required	Quality of Protection(QoP) metric
Modification	Yes	Yes	Yes	Yes	Yes	Yes
Impersonation	Yes	Yes	Yes	Yes	No	Yes
Fabrication	Yes	Yes	Yes	Yes	Yes	Yes
Wormhole	No	Yes	No	No	No	No
Selfish Nodes	No	No	No	No	Yes	No

TAODV uses trust levels whereas all other protocols employ cryptographic techniques. Cryptographic techniques ensure an increased level of security but suffer from increased message sizes and computational overhead. Furthermore cryptographic techniques ensure that the message is not tampered but are extremely vulnerable to Denial-of-Service attack. Trust based protocols provide weak preventative security and the arguments in their favour have been entirely theoretical or simulation based. As we can observe no protocol is able to provide protection against all possible attacks.

VI. CONCLUSION

In this paper we discussed the limitations of AODV and DSR on demand routing protocols. We segregated the limitations as those being common to AODV and DSR on account of on demand protocols and limitations specific to each one. Furthermore, we used these limitations to evaluate the security protocols which were developed taking AODV and DSR as the base protocol. We discussed the basic mechanism of each secure protocol and also listed its advantages and disadvantages. Lastly, we compared the protocols discussed before in a tabular form for a better analytical evaluation. The secure routing protocols are resistant to one or more vulnerabilities. Designing a routing protocol resistant to all the threats and vulnerabilities is yet to be accomplished.

ACKNOWLEDGMENT

The author would like to thank **Professor Parul Tomar** for guidance and invaluable inputs throughout the process of writing this paper.

REFRENCES

[1] C. E. Perkins and E. M. Royer. Ad hoc on-demand distance vector routing. In IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, Feb. 1999.
[2] D. Johnson, D. Maltz, Y.-C. Hu, and J. Jetcheva. The dynamic source routing protocol for mobile ad hoc networks. IEEE Internet Draft, March 2001.
[3] Royer, Elizabeth M., and Chai-KeongToh. "A review of current routing protocols for ad hoc mobile wireless networks." Personal Communications, IEEE 6.2 (1999): 46-55.
[4] Kannhavong, Bounpadith, et al. "A survey of routing attacks in mobile ad hoc networks." Wireless communications, IEEE 14.5 (2007): 85-91.
[5] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.
[6] Liu, Y.; Zhang, R.; Shi, J. and Zhang, Y. (2010): Traffic inference in anonymous MANETs. Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 7th Annual IEEE Communications Society Conference, pp. 1–9.
[7] Zapata, Manel Guerrero. "Secure ad hoc on-demand distance vector routing."ACM SIGMOBILE Mobile Computing and Communications Review 6.3 (2002): 106-107.
[8] S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. In Proc. ACM Mobihoc, 2001.
[9] Papadimitratos, Panos, and Zygmunt J. Haas. "Secure routing for mobile ad hoc networks." the SCS Communication Networks and Distributed Systems modeling and Simulation Conference (CNDS), San Antonio, TX, January 27-31, 2002. 2002.
[10] Sanzgiri, Kimaya, et al. "A secure routing protocol for ad hoc networks."Network Protocols, 2002. Proceedings. 10th IEEE International Conference on. IEEE, 2002
[11] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Ariadne: A secure on-demand routing protocol for ad hoc networks." Wireless networks 11.1-2 (2005): 21-38.
[12] Abusalah, Loay, AshfaqKhokhar, and Mohsen Guizani. "A survey of secure mobile ad hoc routing protocols." Communications Surveys & Tutorials, IEEE10.4 (2008): 78-93.
[13] Li, Xiaoqi, Michael R. Lyu, and Jiangchuan Liu. "A trust model based routing protocol for secure ad hoc networks." Aerospace Conference, 2004. Proceedings. 2004 IEEE. Vol. 2. IEEE, 2004.