Security Enhanced Routing for VANETs

Mohamed Azab, Bassem Mokhtar

Abstract— Vehicular Ad hoc NETworks (VANET) aim to efficiently distribute and transfer information between communicating vehicles or between these vehicles and roadside units. Secure multi-hop routing is critical for communications in the primarily infrastructure-less VANETs. Various routing protocols have been tested on VANETs including proactive (e.g. Destination Sequenced Distance Vector DSDV), reactive (e.g. Ad hoc On demand Distance Vector (AODV)) or hybrid routing protocols. In this paper, we propose and evaluate simple, lightweight security extensions for two topology-based routing protocols, namely AODV and DSDV. These extensions provide authenticity and integrity for routing information with minimal increase in the computation and communication workloads. Simulated studies showed the positive effect of the proposed approach enhancing the routing information security against manipulations securing the entire end-to-end communication.

Index Terms— Vehicular Ad hoc Networks, Routing Protocols, Security Threats, Trust Management, Information Security.

1 Introduction

VANETs are a subclass of MANETs (Mobile Ad hoc NETworks). They have negligible limitation on resources of vehicular nodes and these nodes can move with high speeds. VANETs have unfixed or no infrastructure. These networks emerged to provide comfort and flexible services and information for passengers along their way. VANETs have different communication patterns that can be Peer-to-Peer (P2P) or multi-hop communication.

VANETs are also called Inter-Vehicle Communications (IVC) or Vehicle-to-Vehicle communications (V2V). It has some applications like cooperative traffic monitoring, collision prevention, weather forecasting, and broadcasting information like advertisements for some goods and online services. These varieties of applications lead to call these networks Intelligent Transportation System (ITS) [1].

VANETs mainly depend on multi-hop wireless communication. Topology based routing protocols can be applied whether proactively or reactively. Proactive routing protocols depend on having up-to-date routing information about the communicating nodes in advance in order to route data to any other nodes in the network. DSDV is an example for proactive routing protocols that can be applied for multi-hop wireless ad hoc networks. AODV is one of the on-demand (reactive) routing protocols which can be applied also for multi-hop wireless ad hoc networks.

Both AODV and DSDV are routing protocols that depends on the availability of routing information registered in the routing table at each node. Such information can easily be changed and updated by malicious parties [11,12]. Crucial values such as packet sequence numbers and hop count values can interrupt the entire communication. Cryptographic techniques can be used to prevent the manipulation of these entries by malicious nodes[4-7]. These techniques aim at inhibiting malicious nodes from sending incorrect RREQ or RREP packets including large sequence numbers and small hop count values. Consequently, wrong routing information will be updated in nodes. In addition, malicious nodes can induce route disruption destroying the integrity of data between communicating nodes completely. Attacks such as grayhole attack (dropping randomly some of transmitted packets), blackhole attack (dropping transmitted packets completely), and wormhole attack (tunneling of transmitted packets through a different route) are examples for such attack.

Secure routing protocols are needed to insure node authentication and control packets protection using encryption techniques [10,11]. Symmetric key cryptography is the most commonly used technique to secure such packets [9]. Secure routing protocols must protect mutable information in its control packets to prohibit malicious nodes from broadcasting incorrect routing information for other nodes. Additionally, it should prevent packet spoofing and drooping attacks.

To this end, this paper presents a secure routing protocol that applies symmetric key cryptography for two routing protocols as a simple security extension with low computational-load, small end-to-end delay and high data delivery efficiency. In this work, we assumed tamper resistance vehicular nodes in a VANET.

Some work has been done in this area for securing routing protocols for VANETs or MANETs, with some limitations. One of those limitations was providing security for data or control packet without any assurance for correct node-authentication. A lightweight authentication mechanism is necessary in many applications to authenticate the source to destination communication. In this work, we propose two security extensions for two topology-based routing protocols AODV and DSDV in order to provide data security, integrity, and authenticity.

Due to the variation in network configuration and working conditions for VANETs, we provide two implementations for our extension for both AODV and DSDV. These different implementations provide variable levels of scalability and security. We noticed that the number of simulation scenarios in the validation section of [4] and [8] was not enough to make a fair judgment on the overall performance of the proposed solution. We applied different simulation scenarios with variable

- *Mohamed Azab is currently a Researcher in IRI, The City of Scientific Research and Technological Applications, Egypt.*
  E-mail: mazab@vt.edu
- *Bassem Mokhtar is currently an Assistant Professor in Department of Electrical Engineering in Alexandria University, Egypt.*
  E-mail: bmokhtar@alexu.edu.eg

node speed and direction. Also, we tested this approach on different numbers of nodes to measure the overall performance of the network in different operating conditions.
In the results and discussion section, we compared the overall performance for the whole extension for both protocols against their less-secure counterpart.

By comparing the results of these extensions with those from [4] and [8] using simulation scenarios close to their scenarios, we found that our extensions outperform their work in a considerable amount, whether in dropped to sent packet ratio or in end-to-end delay for AODV, with and without the existence of malicious nodes. In addition, our extension provides better results with more added functionalities.

The remainder of the paper will be as follows. Section 2 provides a background for AODV and DSDV. Section 3 presents our secure AODV and DSDV routing protocols, and the malicious agent. Section 4 describes the simulation scenarios. Section 5 shows results and discussion. Section 6 summarizes some related works. Section 7 concludes the paper.

2 Background

As we mentioned before that AODV and DSDV are two routing protocols that can be applied for multi-hop wireless ad hoc networks. In DSDV, each node has a routing table which contains number of hops for other nodes, identifier of destinations, the identifier of next hop for each destination and its recent sequence number (which refers to the last state of a certain node that it may have new information in its routing table). Each node will update its information about another node if it receives an update packet (periodically sent) includes a sequence number greater than its registered one. Also, the update will be done if the received sequence number is the same as the registered one and the number of hops to that node is less than the recorded value. DSDV uses sequence numbers to minimize routing loop and count-to-infinity problem [2].

AODV differs from DSDV since each node establishes a path to a certain destination when it is required that it is not made in advance. AODV is like DSDV in having routing table for each node. But the entry inside tables is updated on demand. The routing table contains identifier of destinations, number of hops for each destination, the identifier of next hop for a certain destination, list of nodes' identifiers (precursor list) that forward control packets for a destination, and the recent received sequence number for the destination. In AODV, the routing information is updated in routing tables as in DSDV.

AODV has three phases which are route discovery, data transmission, and route maintenance. In the route discovery phase, each node has to flood a Route REQuest (RREQ) packet if it is required to forward data packet to an unknown destination for it. The route request packet has an identifier to prevent duplication at nodes. Nodes, which receive that request packet and have information, will send a Route REPly (RREP) packet through the defined route from which it receives the RREQ packet. On the other hand, if the node has no information about the required destination, it will broadcast RREQ packets to its neighbors. In the phase of data transmission, the nodes will transmit packets through registered information for the required destination in its routing table. If a node detects that there are some broken links for some destinations, it will not have the ability to forward data packets through these links. Hence, it will update its routing table for these destinations marking them as unreachable and send Route ERRor (RERR) packets for nodes in the precursor list [3].

3 Security extensions to AODV and DSDV

We made extensions for AODV and DSDV routing protocols to provide secrecy and authentication against non-legitimate nodes in a VANET. These extensions were tested using network simulator ns-2 (version 2.26). We made these secure extensions to authenticate broadcasting control packets and prevent manipulation of mutable information inside these packets like sequence number and hop count value. Furthermore, the extensions provide data authenticity and integrity between the communicating nodes. We applied a symmetric cryptographic technique for encrypting sequence numbers and hop count values in the headers of transmitted control packets. This encryption scheme depends on symmetric keys shared between the communicating vehicular nodes. This scheme and any another scheme, which depends on a symmetric key cryptography, can be used since it simplifies the simulations and minimizes the computational loads. We assumed that we have tamper resistance nodes, where nodes are preloaded with unique table of keys that will be used for encryption and decryption processes. Each key has a single index which is transmitted in the control packet's header. Each legitimate node can get the key used for encryption, and use it for decrypting the header. The used key is chosen randomly by every transmitting node in order to resist the possibility of a successful brute force attack by an eavesdropper.

We used a hashing mechanism to insure the validity of the received data. The system also has two authentication techniques that suit different working environment. One of which we call it the non scalable approach which assumes that there is a setup phase for the network where all legitimate nodes fill a MAC (Media Access Control) table with all MAC's of each other, and this table (which contains MAC addresses for all legitimate nodes in a network) of MAC's is checked upon the receiving of any new packet against a dedicated field that is added to the packet header to hold the MAC of the sender. This field is encrypted by one of the keys in the key table that is preloaded in all nodes. An index is sent to indicate the encryption key used for each packet. We intended to use the same key for encrypting the sequence number and hop counts to guaranty that any packet retransmission by an attacker will hold old information and the packet will be dropped by the protocol itself. The reason for calling this scheme a non scalable approach, is that in case of adding new nodes all other nodes should notify this node with their MAC and it should broadcast it's MAC to them too, which will cause too much overhead. Another approach which we call it the scalable approach that uses a preloaded signature that will be encrypted and sent in each packet with the same mechanism mentioned before and each node will check for this signature to authenticate the packet before any further processing. This approach needs no reconfiguration upon the addition of any new nodes which is the reason for calling it a scalable approach. The next section will give a quick overview of the hashing and the encryption phases.

3.1 Hash Function

We used a simple hashing algorithm to get hashed value from a string of plain text. The hash value will be attached to the packet header for data integrity checking. At the other end of communication, after decryption, the decrypted text will be hashed again to get new hashed value. This new hashed value will be compared to the value attached within the packet header. If they are equal, the data integrity is assured and decrypted text is accepted; otherwise the packet will be discarded. The algorithm for the hash function can be any type of hashing algorithms like SHA-1or MD5. Because the shortage of time and the complexity of those algorithms, we chose to implement very simple polynomial algorithm.

3.2 Encryption/Decryption Functions

For encryption and decryption feature, we implemented symmetric key cryptography with pre-shared key. These cryptographic functions take input as a string of plain text and shift the ASCII value of each character in the text three positions. Any encryption/decryption algorithm with symmetric key can be implemented here as we mentioned. Some examples for encryption/decryption algorithms that can be implemented are DES, 3DES, EAS, Blowfish.

Fig. 1. The Pseudo Code of the Implemented Extension of the Encryption/Decryption Algorithm

The pseudo code, shown in Figure 1, illustrates the main algorithm for the implemented extension. Furthermore, for testing purposes we have implemented an agent for a malicious node that it has the capability of dropping all packets (makes a black-hole attack) or randomly chosen packets (makes a gray-hole attack).

Another implantation aimed to design a malicious node that will send messages with wrong key which will lead to the drop of these packets at the receiver side .also we implemented a malicious agent which can spoof identifiers of legitimate nodes and intentionally drop any received packets.

4 Simulation scenarios

We tested different scenarios to evaluate the performance of our secure extensions for AODV and DSDV routing protocols with the unsecure versions. So, we have four routing protocols. We used the average end-to-end delay, dropped to sent packets ratio, and average processing time of intermediate nodes as performance metrics. The various scenarios depend on changing number of nodes, speed of nodes, and the percentage of malicious nodes in the network. The simulation model we used for testing uses the IEEE 802.11 MAC protocol with a fixed data rate of 11Mb and 1 Mb for control packets. we also used the OmniAntenna as our antenna model and 20 seconds as our simulation duration. In-order to build a scenario close to the nature of VANETs we randomly set the initial distribution of nodes and set a dedicated path for some of the nodes toward their destinations. By doing so, we were able to test the node interaction and cooperation in delivering the data for long distant destinations. We used the TCP (Transport Control Protcol) protocol with window size of 20 and an ideal time of 1800 ms and burst time of 500 ms and a 32 byte packet size. We used FTP as the running application on the moving nodes. Furthermore, we implemented CESAR cipher with pre-shared key of 3. The following is the list of changes that has been used to illustrate different scenarios for different working conditions for the VANETs. Figure 2 shows the network layout for 100 nodes with 20 malicious nodes.

Scenario (1): a network is established from different numbers of vehicular nodes which are 10, 20, 30, 50, and 100 nodes. We assumed that all nodes have same speed. In each run, we compared between the performance of each routing protocol and its secure version.

Scenario (2): we made the evaluation in this scenario with the 100 nodes. But, we allowed different speeds in that group of nodes.

Scenario (3): different numbers of malicious nodes {5, 10, 15, 20, 25, and 30} are applied in a network size of 100 nodes

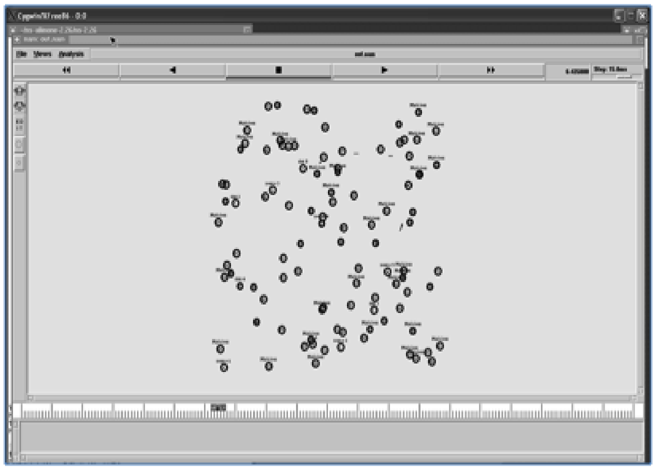

Fig. 2. The Simulated Network Layout

moving with different speeds.

5 Results and Discussion

Due to the increase of the header size caused by the addition of encryption and hashing fields in the header of the control packets of the secure AODV, the intermediate nodes between the communicating pairs in a VANET take more processing time to decrypt those encrypted fields and to compare the hash values in each received packet. Also the results show an increase in the processing time as the number of nodes increases because the path between two communicating nodes may have many intermediate nodes and hence much processing time.

In-order to test the effect of the node speed on the processing time of both AODV and SADOV we carried-out multiple simulations with different node speed of 100 nodes. The results shown in Figure 4 prove that there is much processing time in secure AODV than unsecure AODV especially in large number of nodes. Due to the variation of nodes' speeds, the processing time may have a value less than the one of unsecure AODV as depicted in Figure 3 at a speed of 10. The reason for this case is that the motion of nodes may lead to have a shorter path between two communicating nodes including small number of intermediate nodes and consequently little processing time. For unsecure and secure DSDV scenarios, no processing time was detected. The reason for that was that DSDV is a proactive routing protocol where routing tables are built in advance of communication. Consequently, the nodes consume very short time (can be negligible) to pass the transmitted packets to the next node along the path to the required destination.

The other performance metric tested was the average end-to-end delay for all communicating nodes. First, all the scenarios has been tested for the four protocols unsecure AODV, unsecure DSDV, secure AODV, and secure DSDV. The simulation scenarios handle different numbers of vehicular nodes. Figure 5 illustrates that the secure AODV did not cause much end-to-end delay as unsecure AODV. This might be the result of the light weight encryption scheme that we used. Also, the behavior of secure DSDV is better than secure AODV with respect to the end-to-end delay values. We can notice from the figure that the end to end delay values for both secured and unsecured DSDV are close to each other, which indicates the efficiency of the security mechanism. Also we can see from Figure 6 that the secure version

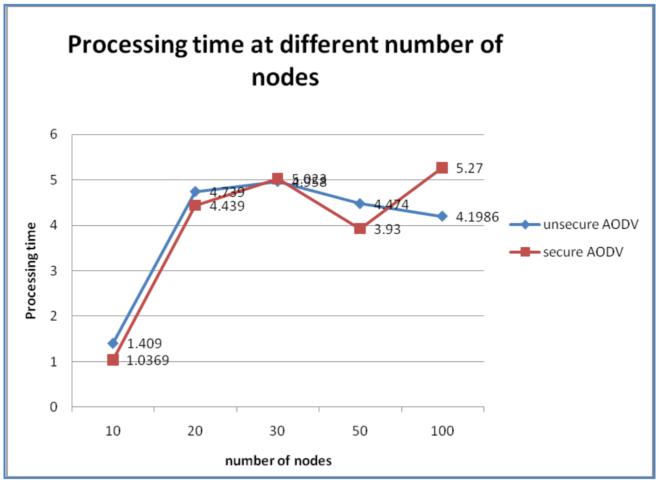

Fig. 3. The Processing Time at Different Number of Nodes

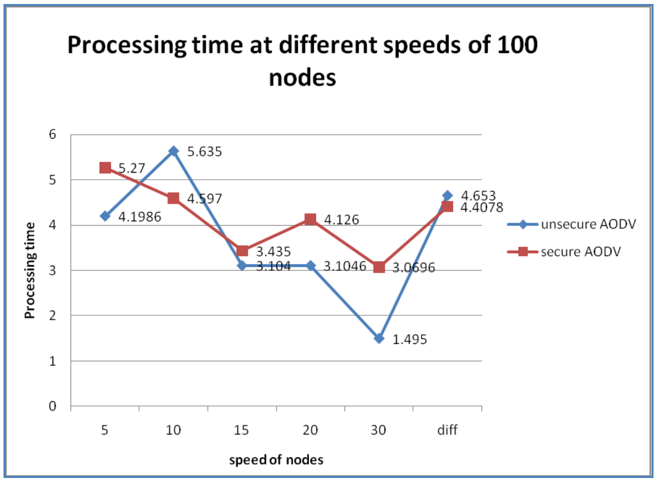

Fig. 4. The Processing Time at Different Speeds of 100 Nodes

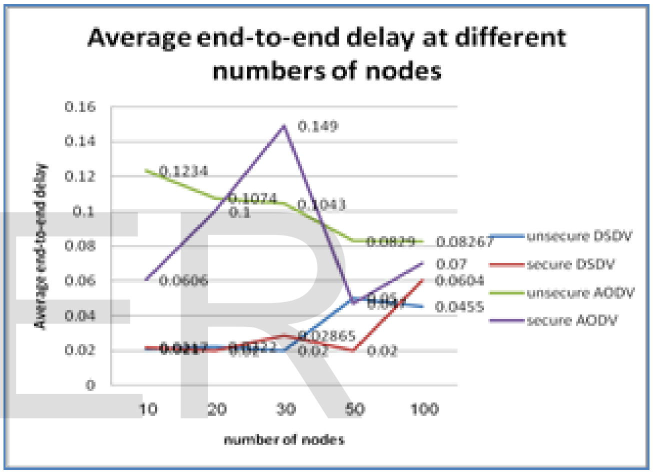

Fig. 5. The Average End-to-End Delay at Different Number of Nodes

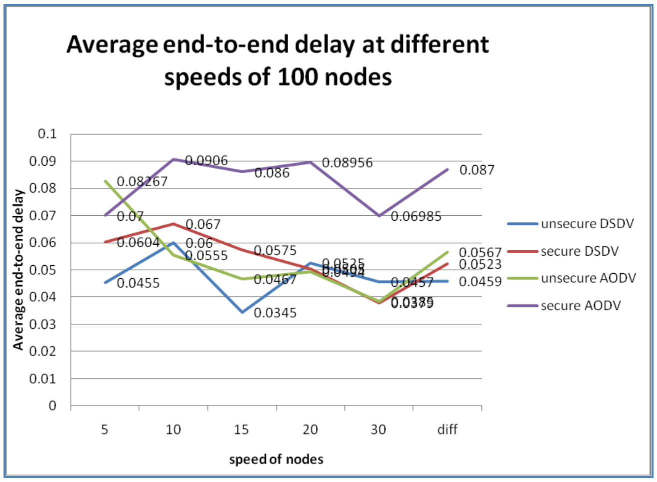

Fig. 6. The Average End-to-End Delay at Different Speeds of 100

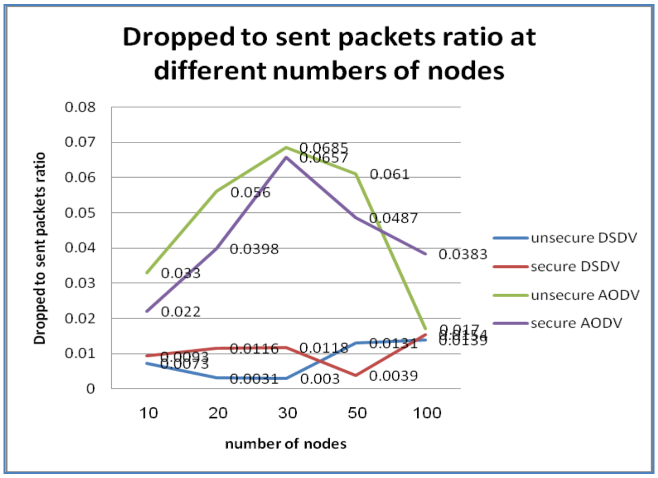

Fig. 7. The Dropped Packet Ratio at Different Number of Nodes

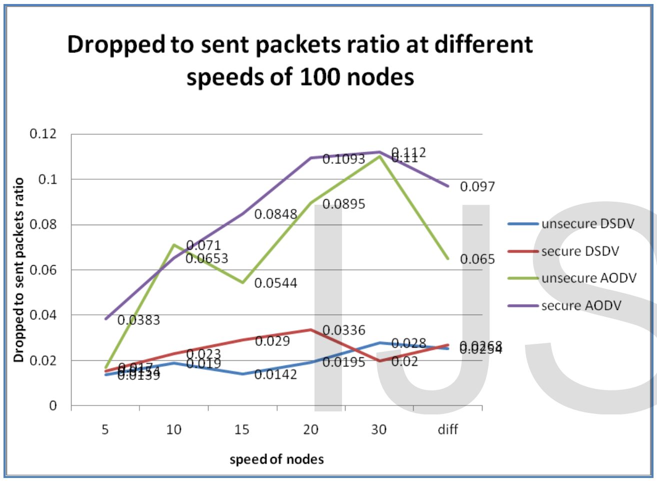

Fig. 8. The Dropped Packet Ratio at Different Speeds of 100 Nodes

shows a better performance than the unsecure version due to the bay bass of the non legitimate nodes in the route discovery phase.

We made other test runs for the four routing protocols at 100 nodes with different speeds as shown in Figure 6. We considered in each simulation same speed for all nodes and we applied different speeds at the last simulation. The obtained results show that the secure AODV has more end-to-end delay than other routing protocols. The reason for that might be caused by the change of speeds that may lead to a route disruption which will increase the end of end delay because nodes will enter a search phase to find a more suitable path for the required destination. Also, the secure DSDV has larger values for the end-to-end delays than the unsecure DSDV this cost manly come from the increased computation time and the communication overhead by the extension of the header size.

We considered the third performance metric which is the ratio of dropped to sent packets. We used this metric to evaluate the overall behavior of the studied routing protocols. In Figure 7, we made different simulations for the four routing protocols at different numbers of nodes. We got good behavior for secure AODV verses unsecure AODV. Also, we got close results with secure DSDV verses unsecure DSDV.

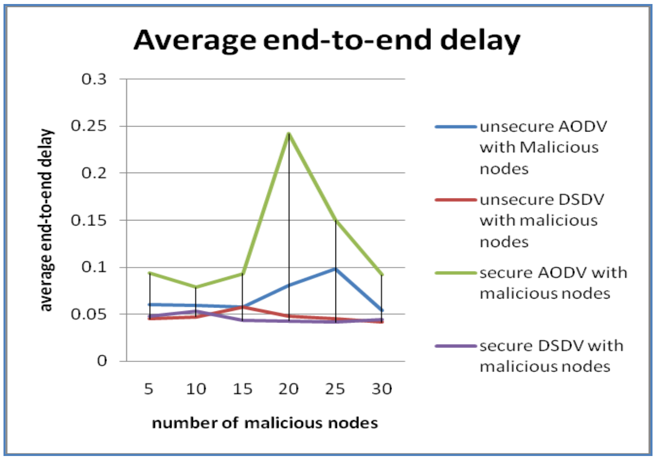

Fig. 9. The Average End-to-End Delay at a Network of 100 Nodes with Malicious Nodes

In Figure 8, the secure AODV has larger ratio than in unsecure AODV since there is an increase in the speed for all nodes which leads to larger possibility of having disruption in routes. We also tried to test the effect of different node speeds within the same network, this scenario leads to better ratio of the sent to dropped packets, the reason for that was the effect of different node speeds added more chance of establishing better routing paths with lower number of hops.

Figure 9 illustrates the effect of the existence of malicious nodes in a network of 100 nodes against the four routing protocols. The figure shows that there is an increase in the delay effect in case of secure routing protocols with malicious nodes that caused by the effect of new secure route establishment away from the path that includes theses malicious nodes. In DSDV the effect was a little bit different due to the nature of the protocol itself because the route establishment is created once and saved in the node routing table, the effect of malicious nodes only appears on update messages which causes much less overload than the way this situation handled by the AODV. Also we can see that the difference between the end-to-end delay values with and without malicious nodes is big enough to be used as a factor of detection

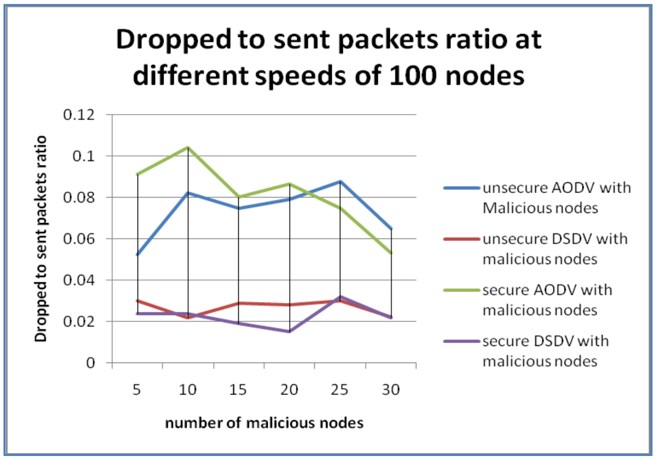

Fig. 10. The Dropped Packet Ratio at a Network of 100 Nodes with Malicious Nodes

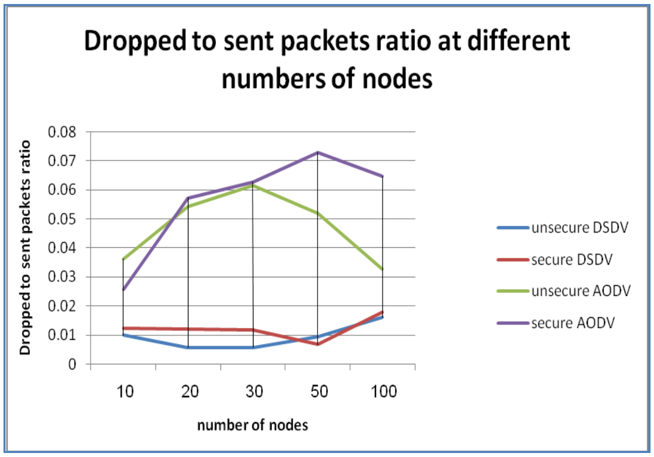

Fig. 11. The Dropped Packet Ratio at Different Number of Nodes with the Existence of Malicious Nodes

of such malicious nodes in the network. This is effect is so clear in Figures 5 and 9 for the behavior of the secure AODV routing protocol at 100 nodes.

Figure 10 illustrates the effect of the existence of malicious nodes on the dropped to sent packets ratio at a network of 100 nodes. The figure shows that by the increase of the number of malicious nodes, the secure protocols succeeded to establish more stable routing paths away from those malicious nodes which enhanced the drooping to sent packet ratio to a reasonable extent. Then, we made two runs to test the effect of different transmission loads at the communicating nodes on the ratio of dropped to sent packets.

In Figures 11 and 12, we tested the increase of load on the dropped to sent packet ration but it remains the same which indicates the stability of our implementation under different loads where the amount of dropped to sent packet does not significantly increase by different amounts of load.

6 Related Work

We made performance evaluations for two topology based routing protocols (AODV and DSDV) and their secure extensions. We made our own secure extensions by encrypting the sequence numbers and hop count values in the header of the control packets using symmetric key cryptography. Also, we applied a hashing function for sequence numbers and hop count values before encryption and decryption process to check-on the correctness and validity of the control packets. We used the average end-to-end delay, processing time, and ratio of dropped to sent packets as our performance metrics. There are other related works which evaluated the performance of reactive and proactive topology based routing protocols using different performance metrics.

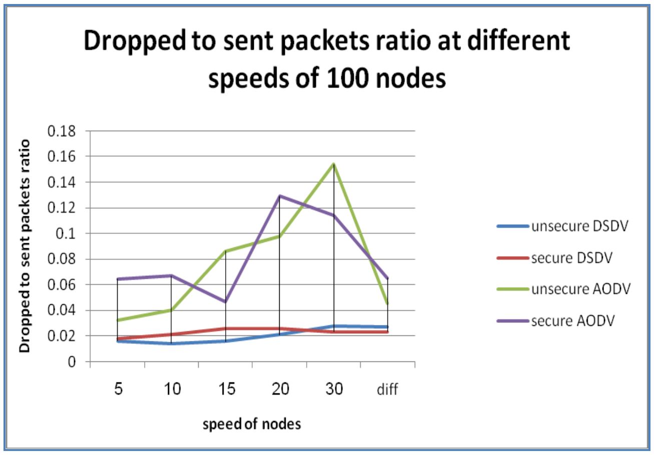

Fig. 12. The Dropped Packet Ratio at Different Speeds of Nodes with the Existence of Malicious Nodes

In [4], the authors applied some security extensions to the AODV routing protocol. They modified the AODV routing agent implemented in ns-2 using symmetric key cryptography. The extended SAODV was applied only for routing messages. They considered a single (group) key for each group of nodes updated before communication between nodes. This SAODV depends on computation of message authentication code using the symmetric shared key. Also, a publically known hash chain of fixed length suitable for the network size is used by every legitimate node along a path that that node can reveal the correct hash value. This value is used to protect the mutable fields (sequence numbers and hop count fields) and it is appended in the header of the routing message. The security extension for AODV protects the increasing of the sequence number value and decreasing of the hop count value. Furthermore, SAODV uses digital signatures computed by the symmetric key to protect the non-mutable fields like the node identifier. They used also the implementation of Monarch project for Ariadne routing protocol with ns-2. They evaluated the two routing protocols with performance metrics (end-to-end delay, route acquisition time, and protocol load) rather than security metrics (time required to discover the used key by different number of malicious nodes). They made simulations with respect to two parameters which are number of nodes and their speed. The results showed that the SAODV performs better in networks of small number of nodes with low speeds. Ariadne showed a higher overhead in small number of nodes but it is much better in case of large number of nodes with high speeds. We got small end-to-end delay values for our secure AODV than the secure AODV implemented in [4] at different numbers of nodes at speed of 5 m/sec. In addition, we tested the effect of higher and different speeds for communicating nodes.

Applying authentication techniques via digital signatures with the usage of AODV routing protocol in VANETs can help strengthening the security of data messages [13].

In [5], AODV, DSDV, and DSR (Dynamic Source Routing) were evaluated through different scenarios considering two radio models which are Two-Ray-Ground and Shadowing in an ad-hoc sensor network. The authors generalized the radio model by allowing path loss randomness in the service environment of the network. Packet repetition transmission is used as a technique for congestion control. The repetition rate depends on bound for signal distortion perceived at a sink node. The authors analyzed the radio irregularities relying on this technique. They used ns-2 as the network simulator and packet delivery ratio as a metric for evaluation. The results showed that the shadowing, which destroyed the regularity of a network, decreases mean distances between nodes and increases the latency of packet transmission. Also, DSDV behaved worse in case of Two-Ray-Ground model than DSR and AODV. But, DSDV behaved better in the shadowing model.

In [6], the authors made performance evaluation for AODV, DSR, and DSDV routing protocols using network simulator ns-2. They simulated different scenarios characterized by mobility, load, and size of the ad hoc network. They used Rice Monarch project with their ns2 extension for simulation. Packet delivery fraction, average end-to-end delay, and routing load were used as performance metrics. The results showed that AODV and DSR behaved better than DSDV in high mobility simulations.

Different simulation scenarios were done for AODV and DSDV routing protocols in [7]. The authors considered various speeds of nodes in MANETs to evaluate the performance of the two routing protocols. They made four mobility models which provide different speeds for nodes.

Three performance metrics were used which are packet delivery fraction, average end – to – end delay, and routing overhead. The obtained results indicated that AODV has an end - to - end delay lower than DSDV. But, AODV has a protocol overhead larger than DSDV.

Quantitative performance comparisons were done between AODV and SAODV in [8]. Small-scale experiments were done using laptops in indoor and outdoor environments that some impairments like multipath fading was studied to quantify its effect on the two studied routing protocols. The authors tested the effect of extra control overhead and related processing upon UDP and TCP traffics. The used SAODV routing protocol is as mentioned in [4] that digital signatures and hash chains are used to protect non-mutable and mutable fields respectively. The results clarified that SAODV was effective in routing manipulation and packet dropping attacks. We had improvements in values of dropped to sent packets ratio [i.e. (1 - packets deliver ratio)] compared with results obtained at different sessions in [8] whether with or without malicious nodes. In [14], authors proposed a routing strategy based on double acknowledgement packets to detect and to identify malicious nodes in VAENTs. However, such routing approach might increase the packet delivery delay and lead in quality of service (QoS) deterioration, especially, in high speed applications. Other research works in literature formulated optimization problems for providing secure routing for VANETs considering multiple QoS constraints [15].

7 Conclusion

Routing protocols in highly dynamic ad-hoc networks as VANETs have a major role in achieving the goals of these networks. These routing protocols have vulnerable mutable information that if tampered-with, may drastically impede network functionalities. Hence, secure extensions should be applied for routing protocols to protect their role from any misbehaved nodes and effects. We applied a novel secure extension using symmetric key cryptography and a hashing function for two topology based routing protocols AODV and DSDV. We evaluated the performance of our secure versions of those routing protocols against their original unsecure versions using average end-to-end delay, processing time, and ratio of dropped-to-sent packets ratio as performance metrics. We made different runs by changing network size (number of nodes) and speed of nodes.

The implementation of cryptographic mechanisms showed a very small effect at the processing time of the intermediate nodes. This means that our secure extensions approximately do not impact upon the overall behavior of AODV routing protocol. Consequently, our extensions do not cause much change in the size of the control packets headers of the routing protocols.

The overall behavior of these secure versions has a comparable efficiency to the unsecure versions as shown in graphs of dropped to sent packets ratio. Adding malicious nodes to the network increases the average end-to-end delay in secure AODV because of their malicious behavior which results in prolonging the time required to have secure paths between source/destination pairs.

Some future issues can be discussed and implemented as applying malicious agents who have the capability of making identifier spoofing and directed functions as misrouting data packets to specific nodes in the network. Also, other cryptographic mechanisms and key management systems can be tested and compared with our secure extensions which might lead to an optimized cryptographic mechanism. This mechanism can be used with routing protocols to achieve a balance in the tradeoff between data authenticity and integrity, and overall performance of those routing protocols.

References

[1] F. Li, and Y. Wang, "Routing in vehicular ad hoc networks: A survey", IEEE Vehicular Technology Magazine, Volume 2, Issue 2, June 2007 pp. 12 – 22, 2007.

[2] M. A. K. Khattak, K. Iqbal, and S. H. Khiyal, "Challenging Ad-Hoc Networks under Reliable & Unreliable Transport with Variable Node Density", Journal of Theoretical and Applied Information Technology, vol. 4, no. 4, pp. 309 -318, 2008.

[3] O. Abedi, M. Fathy, and J. Taghiloo, "Enhancing AODV Routing Protocol Using Mobility Parameters in VANET", International Conference on Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS March 31 - April 4 2008 pp. 229 – 235, 2008.

[4] Haiqing Liu, Licai Yang, Yao Zhang, "Improved AODV routing protocol based on restricted broadcasting by communication zones in large- scale VANET", Springer, pp. 857-872, 2015.

[5] Iqbal, F., et al. I-AODV: Infrastructure based Ad Hoc On-demand Distance Vector routing protocol for Vehicular Ad Hoc Networks. in Smart Instrumentation, Measurement and Applications (ICSIMA), 2013 IEEE International Conference on. 2013: IEEE.

[6] S. Shah, A. Khandre, M. Shirole, and G. Bhole, "Performance Evaluation of Ad Hoc Routing Protocols Using NS2 Simulation", Mobile and Pervasive Computing (CoMPC–2008), 2008.

[7] Shams-ul-Arfeen, A. W. Kazi Jan M. Memon, and S. Irfan Hyder, "Performance Evaluation of MANET Routing Protocols Using Scenario Based Mobility Models", Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, 419–424, 2007 Springer, 2007.

[8] A. Dua, et al., "A systematic review on routing protocols for vehicular ad hoc networks," Vehicular Communications, vol. 1, pp. 33-52, 2014.

[9] Seyed Mohammad Safi, Ali Movaghar, Misagh Mohammadizadeh, "A novel approach for avoiding wormhole attacks in VANET", in First Asian Himalayas International Conference on Internet, 2009, pp. 1-6.

[10] Irshad Ahmed Sumra , Jamalul-lail Ab Manan , Halabi Hasbullah, “Timing Attack in Vehicular Network”, in Recent Researches in Computer Science, 2011, pp. 151-155.

[11] TamilSelvan, Komathy Subramanian, Rajeswari Rajendiran, “A Holistic Protocol for Secure Data Transmission in VANET”, in International Journal of Advanced Research in Computer and Communication Engineering, 2013, pp. 4840-4846.

[12] B. Mokhtar and M. Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," Alexandria Engineering Journal, vol. 54, pp. 1115-1126, 2015.

[13] K. Ravi and K. Praveen, "AODV routing in VANET for message authentication using ECDSA," in Communications and Signal Processing (ICCSP), 2014 International Conference on, 2014, pp. 1389-1393.

[14] R. Jahan and P. Suman, "Detection of malicious node and development of routing strategy in VANET," in Signal Processing and Integrated Networks (SPIN), 2016 3rd International Conference on, 2016, pp. 472-476.

[15] M. H. Eiza, et al., "Secure and robust multi-constrained QoS aware routing algorithm for VANETs," IEEE Transactions on Dependable and Secure Computing, vol. 13, pp. 32-45, 2016.