A Trust Based Mutual Authentication and Data Encryption Scheme for MANET Security

Mansoor Ihsan(✉) and Martin Hope

The University of Salford, Manchester M5 4WT, UK
{m.ihsan1,m.d.hope}@salford.ac.uk

Abstract. MANET are self-configurable wireless network where the nodes do not have fixed infrastructure, no centralized mechanism, nodes are fully cooperative, highly mobile and dynamic. There is no inherent security between the nodes for secure communication and data exchange. One of the huge security challenges is authentication of nodes in such environment in general and peer communicating nodes in particular where nodes are communicating for the first time.

The proposed scheme presents a novel solution to authenticate peer nodes (source and destination) with no prior trust and security associations. As no pre-established trust exists before the MANET is initialized therefore, in MANET, nodes present a huge challenge of authenticating communicating peer nodes. The proposed scheme provides a solution to authenticate the sending and receiving nodes using trust based scheme as the sender and receiver doesn't have first-hand information about these trust values as they could be at the opposite end. Thus, the trust is calculated by nodes for all their neighbours and is send to peer communicating nodes when requested before peer nodes initiate communication. We refer to this process as authentication through trust. Lastly, to ensure end to end data encryption, the mutual trust scheme is combined with Diffie-Hellman Elliptic Curve DHEC Key Exchange. This allows nodes pair to exchange data securely by using shared secret keys to encrypt data.

Keywords: MANET · Network security · Trust-based scheme · Trust-based authentication · Cryptography · Asymmetric key exchange

1 Introduction

One of the vulnerabilities of MANET is the lack of secure communication mechanism between nodes and protection against various threats. The minimum requirement of implementing security in any system is achieving the security goal of Availability, Integrity, Authenticity commonly referred to a CIA. This paper is concerned with the using trust to achieve authentication in MANET nodes. This can only be achieved by forming a secure channel between the communicating nodes. The algorithm used is a combination of trust based scheme as a framework and available efficient cryptographic techniques to achieve the above security goals. The scheme is divided into three steps. The first step of the algorithm is to build the trust factors which provide a secure

M. H. Miraz et al. (Eds.): iCETiC 2019, LNICST 285, pp. 90–105, 2019.
https://doi.org/10.1007/978-3-030-23943-5_7

platform for the later steps of the protocol that uses the trust values to authenticate peer node. Lastly, a secure key management scheme to secure communication between nodes in the network is also proposed to provide data encryption.

The trust calculation can be achieved using any trust threshold scheme proposed [1–7]. Once the trust is established between neighbour nodes, the trust values can be used to validate communicating peer nodes in the second step. The scheme addresses the issue of authenticating peer communicating nodes that could be far apart and one-to-one trust value exchange is not possible. Thus, step-one is a framework to provide the level of security required in the form of a trust and step-two can be used to authenticate nodes based on those trust values.

2 MANET Security Completed Work

Routing protocol in MANETs such as AODV were designed without taken security considerations into account therefore, it is prone to number of security threats as mentioned earlier. There are number of attacks that has been identified and studied in MANET. The type of attack also depends on which network has been targeted. We will discuss more advanced attacks that could affect MANET. Some of the types are Blackhole [7], Greyhole [8], Wormhole [9, 11] that are classed as Denial-of-Service (DoS) attacks. Other types of attacks are Byzantine [12], Flooding [13], Grayhole [10] and Rushing [14].

Extensive research has been done and various security protocols have been proposed by the researchers in an attempt to secure different aspects of MANET. The mobility of nodes and constantly changing topology makes availability challenging in MANET. It is essential to the network operations. MANETs are vulnerable to attack on any level of the open system interconnection OSI model including physical attacks such as Denial of Service DOS or wireless jamming techniques as well as attacks on higher-level services such Key Management services [10]. We will briefly discuss and analyze some of secure routing protocols developed for MANETs such as SAODV [15], SEAD [16], TESLA [17], Ariadne [18], SAR [19], Security Aided Adhoc Routing [20] and ARAN [21].

- Secure Adhoc On-demand Distance Vector SAODV [15] routing protocol is used to secure the routing messages for the original AODV. Basically the SAODV uses digital signature, a branch of symmetric cryptography, to authenticate non-mutable fields and using hashing algorithm such as hash chain to authenticate the mutable field i.e. hop count for both route request RREQ and route reply RREP message [16].
- Authenticated Routing for Adhoc Network ARAN [21] is another type of MANET security protocol that uses digital signatures to protect the non-mutable fields of the routing messages and uses Open SSL library for certification. This is thought to be time consuming and generate a lot of overhead.
- Security Aware Routing protocol SAR [19] is a trust based reactive protocol. It uses trust values and relationships with the nodes which form the basis of its routing

decisions. Only trusted nodes can participate in the routing. The protocol does not provide high-end security.

- Another protocol proposed called Security Aware Aided Adhoc Routing SPAAR [20]. It's a location aware protocol which uses geographical information to secure routing information and uses asymmetric cryptography i.e. the use of public key infrastructure for routing.
- Hu et al. [16] proposed Secure Efficient Ad Hoc Distance Vector SEAD and used a protocol, which is based on the design of DSDV [20]. SEAD is designed to prevent attacks such as DoS and resource consumption attacks. Also uses One-Way Hash Chains to secure routing.
- Ariadne also developed by Hu et al. [17] which is based on the operation of DSR [22]. Ariadne [18] uses message authentication code (MAC) and secret key shared between two parties to ensures point-to-point authentication of a routing message. Ariadne is a secure on-demand routing protocol and uses symmetric cryptographic operations. The protocol provides security against one compromised node and prevents many types of denial-of-service attacks. However, it relies on the Timed Efficient Stream Loss-tolerant Authentication TESLA [17]. This is not suitable for MANET as it requires clock synchronisation.

3 Trust Based Scheme

Trust based routing protocol works by adding Trust parameters to the nodes. Nodes operate in promiscuous mode and hear the conversations between other nodes in transmission range. Trust can be computed by taking into account different factor such as packets sent, received, acknowledged and forwarded by various nodes in the network. Therefore, nodes representing high trust can be selected as best path for communication. Trust schemes are used to mitigate security attacks and identify malicious nodes in the network as an alternative to cryptographic methods due to special characteristics of MANET. Extensive research has carried out on the use to trust threshold schemes in MANET. In the next section we will discuss some of trust based schemes proposed.

Several techniques have been proposed to detect and eliminate malicious nodes in the network such as [23–31]. One of the earliest techniques proposed was Watchdog and Pathrater. The Watchdog technique identifies misbehaving nodes while Pathrater technique calculates path avoiding misbehaving nodes [24]. The Pathrater rates every path in its cache and select a path that best avoids misbehaving nodes. In [27] the author used the concept of incentives called beans to forward packets. Each node in return for participating in packet forwarding earns beans. The packet is automatically dropped when the packet run out of beans. A credit-based scheme known as Sprite was proposed by [30] in which the receipts of all packets send and received are kept and reported to Credit Clearance Services CCS when there is an internet connection. The CCS can make decision based on its report about the individual nodes. Scheme called Ex-watchdog proposed by [32] was proposed to address the weaknesses of watchdog scheme by discovering malicious nodes which can partition the network by generating false reports. Another Intrusion Detection System proposed by [5] relies on watchdog technique to overcome deficiencies in the original watchdog scheme by introducing end-to-end acknowledge called TWOACK. Another trust based scheme called Adaptive Acknowledge scheme (AACK) [27] is an attempt to reduce detection overhead while increasing detection efficiency through detecting misbehaving node rather than link proposed in TWOACK [5]. Muhammad et al. [1] proposed Adaptive Trust Threshold Strategy for detecting and isolating misbehaving node. The main difference between this and other schemes proposed is that it adapts to changes in topology and therefore, its threshold against which the trust is measured and compared is a dynamic value.

Confident scheme was proposed by [26] which is also a reputation based scheme. It has four major components Monitor, Reputation System, Path and Trust Manager. Monitor performs watchdog function, Reputation deals with node rating, path is about path rating and Trust deals with alert messages.

4 Our Proposed Scheme

Trust based routing protocol works by adding trust parameters to the nodes. Nodes operate in promiscuous mode and hear the conversations between other nodes in its transmission range. Trust can be computed by taking into account different factors such as packets sent, received, acknowledged and forwarded by various nodes in the network. Therefore, nodes representing high trust can be selected as best path for communication. Trust schemes are used to mitigate security attacks and identify malicious nodes in the network as an alternative to cryptographic methods due to special characteristics of MANET. Extensive research has been carried out on the use of trust schemes for security in MANET. The next section will discuss some of trust based schemes proposed.

The proposed mutual authentication scheme can be implemented on top of any trust based scheme. There have been number of trust schemes proposed [1–6] that can be used as a framework for the proposed scheme in step-one.

For instance, the Watchdog technique identifies misbehaving nodes while Pathrater technique would calculate path avoiding misbehaving nodes [24] using trust values. Another example of a scheme using static trust is Adaptive Acknowledge scheme (AACK), [27] is an attempt to reduce detection overhead while increasing detection efficiency through detecting misbehaving node rather than link proposed in TWOACK [5]. All these schemes use trust in some shape and form to represent trust in the nodes.

4.1 Neighbour Nodes Trust Calculation

According to the above schemes [1, 4, 6], trust is generally calculated by nodes listening in promiscuous mode to the packets send and received by its corresponding neighbours. Our scheme relies on this information collected by neighbour nodes as being first hand is used to authenticate peer nodes. The trust is represented as Average Trust and calculated using Eq. 1 below.

$$\text{Average Trust T} = \frac{\sum \text{Packets Sent/Recvd}}{\sum TotalPackets} \tag{1}$$

Once the node trust is calculated using trust schemes mentioned above then the trust is compared against an arbitrary static trust threshold to determine the final trust of a node (κTa) using Eq. 2. The Average trust (T) In most of the cases the trust is calculated by neighbour nodes as they operate in promiscuous node and can listen to the packets send and received by its neighbour.

4.2 Mutual Trust Authentication Scheme Structure

We have used AODV as a reference to compare our scheme. AODV is modified to embed our scheme and comparisons are drawn to validate our findings. There are four types of messages RREQ, RREP, RERR and RACK defined by AODV protocol. Our scheme only uses the RREQ message at destination node and RREP at the source node for implementation.

According to this stage, once the Trust values received from neighbors of corresponding peer nodes then, the trust values are combined as shown in Eq. 2, to calculate the peer node trust.

$$\kappa Ta = \frac{1}{N}\sum_{i=0}^{N} \mathrm{T}i \tag{2}$$

Where T is Average Trust value calculated by each neighbor node, N is Total number of neighbors, K is the trust of node a and i is the Node index.

Once the trust values are received from all the corresponding neighbor nodes then the trust values are evaluated to calculate final trust value by using Eq. 2. The peer node is authenticated if the trust threshold is above certain static predetermined threshold or authentication fails if the trust threshold calculated is low. The Algorithm-1, represents how the node trust is calculated using trust based schemes and the node is declared as trust or malicious as a result of the computation. The Algorithm 1 shows how the trust is calculated in the majority of research work presented so far.

```
Begin
Compute Node Trust
Compute Static Trust
        If Node Trust >= Threshold then
               Trusted
   Else
               Not Trusted
End
```

Fig. 1. Trust threshold scheme algorithm

4.3 Mutual Authentication Process at Source Node *S*

The source node S waits for a route reply RREP after sending a RREQ in order to communicate with the destination node D. When it received a RREP from destination node D, the source node S then repeats the same process performed by the destination node. Source node also requests the trust values from all the neighbours of the destination node. Upon receiving the trust values of destination neighbours, the source compares the trust values and authenticates the destination node to establish communication. As both nodes S and D have no security association with one another to exchange data, hence the proposed scheme provides that layer of security by using trust to authenticate destination node. The Fig. 1 shows the steps in AODV, when the Mutual Authentication scheme is implemented and the trust is requested by source node. The steps highlighted in the end, where the source receives the RREP, it requests the trust from destination's neighbours followed by DHEC, which constitutes the last step.

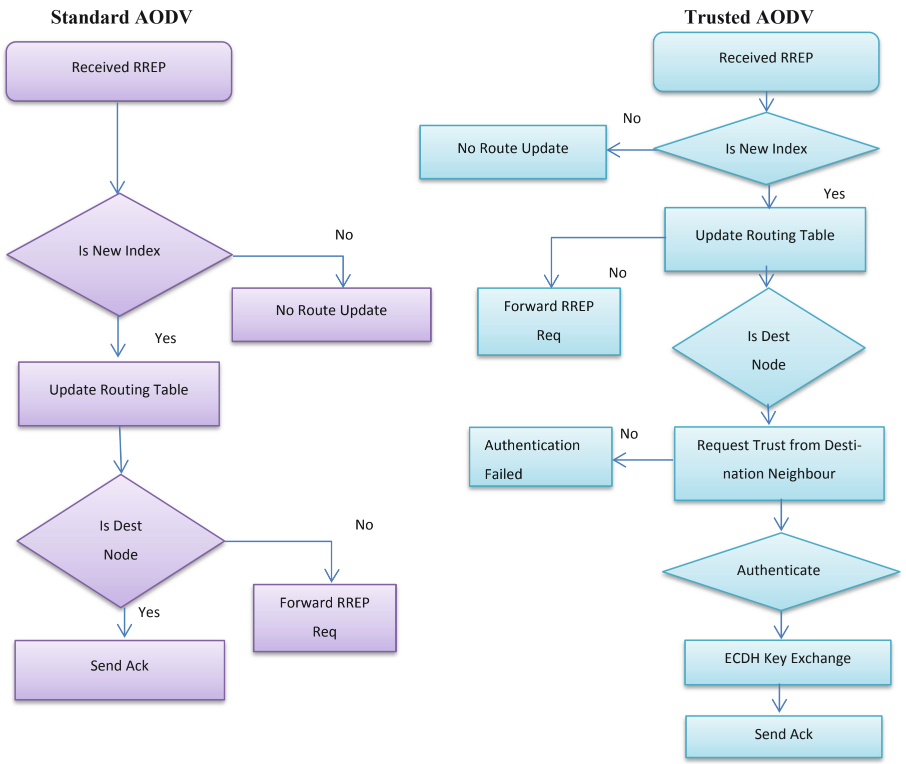

Fig. 2. Source node DFD standard versus mutually authenticated trusted AODV

4.4 Mutual Authentication Process at Destination Node *D*

This section describes how AODV can be used to implement the proposed mutual authentication scheme. When a source node S wishes to communicate with destination

Node D, and doesn't have a route to destination node D, it sends a RREQ. In the normal AODV operation the destination node sends a reply to the source node with the valid root when the RREQ reaches the destination node D and the last action performed is a |Send Reply| message sent. After the AODV operation is complete and before any data communication is performed by both nodes, the authentication and authorization stage begins which concludes the first phase of the proposed scheme.

According to this stage, the destination node requests trust values from source S and all its neighbour nodes. Once the trust values are received from all the corresponding neighbour nodes of S then the trust values are evaluated to calculate final trust value. The node is authenticated if the trust value is equal to and higher than the values received from all neighbours, and authentication fails if the trust value is low. The same process is repeated by the source node S to authenticate destination node by requesting source and its neighbours trust values recorded for the source node.

The AODV process at destination node is shown in Fig. 3. The Fig. 3 presents the difference between standard and AODV process based on Mutual authentication. The authenticated AODV requests the trust values from source neighbour node and if authentication is successful, a reply is sent in the form of RREP message. Before any data is exchanged the DHEC algorithm is implemented. The additional steps are shown at the end of trusted AODV in Fig. 3.

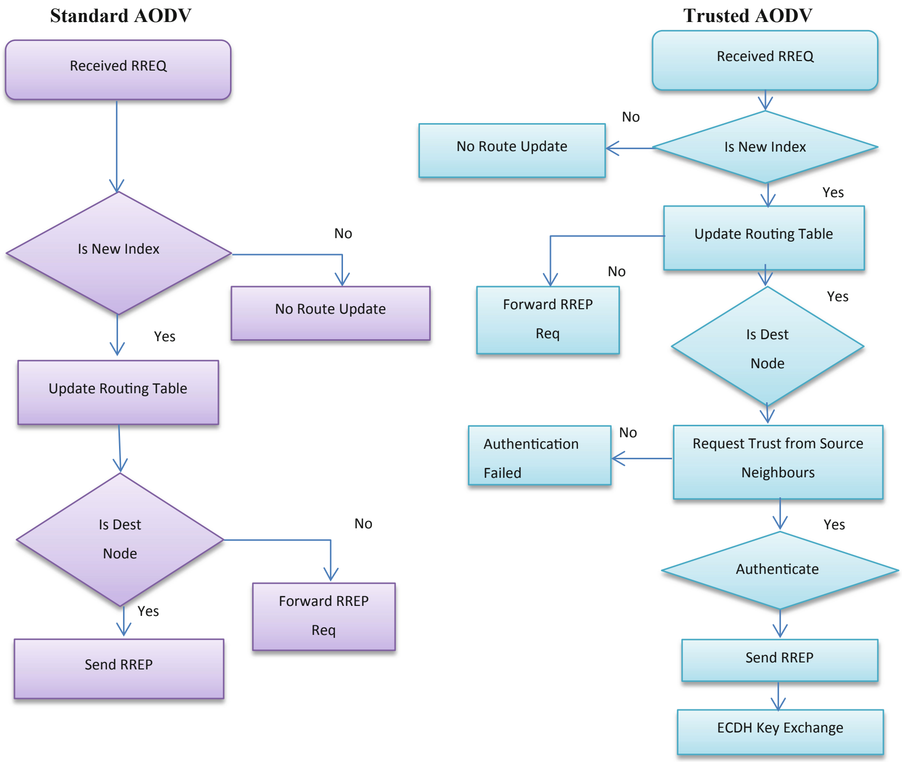

Fig. 3. Destination node DFD standard versus mutually authenticated trusted AODV

4.5 Diffie-Hellman Elliptic Curve Key Exchange

To ensure the data cannot be intercepted by any third party or protect is from eavesdropper, we propose implementing the cryptographic protocol. DHEC algorithm is implemented when Route Request (RREQ) message is received and RREP acknowledgement is sent by the destination node D. This is a novel concept through which peer nodes authenticate one another through trust which is discussed in detail in Sects. 4.3 and 4.4. The authentication using trust ensures that the communicating nodes are trusted and their trust values are endorsed by the neighbour. We believe that trust values calculated by neighbours can have highest level of trust, than trust calculated through other methods. When the trust and mutual authentication schemes are combined they provide a foundation to secure key exchange between any communicating nodes. The secret key could be used to provide security in the following ways;

1. Authentication and authorization
2. Encrypting data exchange between nodes

This could provide protection against the forms of attack that are common in MANET, such as Blackhole, Greyhole, Rushing and Wormhole attack.

The last step of our proposed scheme is the key exchange mechanism to encrypt messages using secret keys. The keys are exchanged using Diffie-Hellman key exchange [31]. This would ensure the data is encrypted and could not be intercepted or tempered with by eaves dropper between source S and destination D.

DHEC scheme allows us to exchange secure information i.e. secret shares between sender and the receiver over insecure channel. This is an example of Asymmetric algorithm [31]. This algorithm states that two nodes exchange public keys and then each performs a calculation on their individual private key and the public key of the other. The result of this whole process gives us an identical shared key. The shared key obtained is used for encrypting and decrypting data between two nodes. The scheme provide a framework about how to perform key generation and exchange between parties or devices that do not yet have secure connection to establish shared keying material (key that can be used with symmetrical keying algorithm such as AES, DES, HMAC) therefore it's more a key-agreement protocol than an encryption algorithm. Elleptic Curve Diffie Hellman is more efficient variant of Diffie-Hellman key exchange algorithm which will be used in our scheme [32]. They are used in Public Key Cryptography for conceiving efficient factorization algorithm.

Public Key cryptography is designed on the principle of hardness of solving the following two problems;

1. Factorization of large integers
2. Discrete Logarithm Problem DLP

The main idea behind the above concept is the trapdoor one way function.

A one way Trapdoor function is such that
Given x, $Y = f(x)$ is easy to compute
Given Y, it's computationally infeasible to calculate x

Elliptic curves are set of points defined by the solution to the following equation

$$E = \left\{(x, y)|y^2 = x^3 + ax + b\right\} \\ a, b \in K \tag{3}$$

Where a is an element of field, b is an elements of field and K is a field.
Some of the fields K that Elliptic curves are defined over are

- R: Real numbers
- Q: Rational Numbers
- C: Complex numbers
- Z: Integers modulo p represented as Z/pZ

Following is the example of a graph of elliptic curve over real numbers R (Fig. 4).

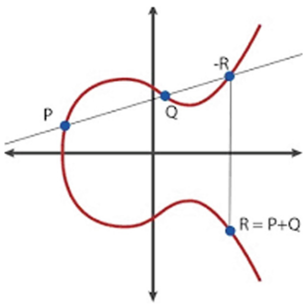

Fig. 4. Elliptic curve over integer modulo p

Also there is a point at infinity represented as O

Point at infinity: O

And there is also a condition that

$$4\,a^3 + 27\,b^2 \neq 0 \tag{4}$$

Discrete Logarithm Problem DLP is a type of one-way function as explained above in which exponentiation is easy but logarithm is difficult to compute. The types of cyclic groups used in public key cryptosystem are
Example of DLP in zp^*

- Given the finite cyclic group zp^* of order p − 1 and a primitive element $a \in zp^*$ and another element $b \in zp^*$
- The DLP is the difficult computation of determining the integer $1 \leq x \leq p - 1$ such that

$$a^x \equiv b\, mod\, p \quad or \quad x = log_a b \tag{5}$$

Elliptic curves uses shorter encryption keys hence consume fewer memory and CPU resources. It offers more security per bit in increase in size and is more computationally efficient then the first generation RSA and Diffie-Hellman public key systems [31]. The figure below shows the comparison of Diffie-Hellman and RSA key exchange protocols using elliptic curve (Table 1).

Table 1. Comparative analysis between RSA and Diffie-Hellman using ECC

Symmetric encryption (key size in bits)	RSA and Diffie-Hellman (modulus size in bits)	ECC key size (in bits)
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

The above comparison shows that the Elliptic Curve keys are much smaller [31]. Secondly the ratio of the key lengths utilizing the protocol from multiplicative group using modulus mod p as shown in the middle table to the key length of Elliptic Curve protocol is increased from 6:1 for 80 bits, 12:1 for 128 bits and 30:1 for 256 bits [33]. This implies that the more security is required the more efficient ECC becomes.

In order to keep the shares confidential and secure so it doesn't get into malicious hands or get compromised in any way during exchange process from Source node to the Destination Node as shown in Figs. 1 and 2 above we propose the use of Diffie-Hellman Elliptic Curve Key exchange algorithm.

The following section describes various steps needed to configure DHEC protocol.

Let E be an elliptic curve over a finite field k.

Let P, Q be points on E such that P = nQ for some integer n.

Let |P| denote the number of bits needed to describe the point P.

We wish to find an algorithm which determines n and has runtime polynomial in |P| + |Q|. So this problem seems hard. This is also referred to as Discrete Logarithm Problem where "adding is easy on Elliptic Curve but undoing is hard" [34].

Using a multiplicative group of points on an elliptic curve the ECDH protocol works as follows;

1. Node A and Node B agree on an elliptic curve E over a Field Fq and a base-point $P \in E/Fq$.
2. A generates a (random) secret kA and computes PA = kAP.
3. B generates a (random) secret kB and computes PB = kBP.
4. A and B exchange PA and PB.
5. A and B compute PAB = kaPB = kbPA

The secret kA and kB is a random value $\in \{1, \ldots, n-1\}$ where n is the order of the group generated by P [36] and exchanged non secure channel without revealing Identity of the secret.

5 Performance Metrics

The performance of the proposed scheme is evaluated using the following metrics:

- **Throughput:** It is the amount of data (bit or packets) transferred between source and destination per period of time (seconds).

$$\text{Throughput} = \frac{Size\ of\ Data\ Received}{StopTime - StartTime} \tag{3}$$

- **Packet delivery ratio:** The ratio at which packets are delivered in the network.

$$PDR = \frac{\sum_{\forall i \in D} TPR_i}{\sum_{\forall i \in D} TPS_k} \times 100 \tag{4}$$

The TPRi represents the total number of packets received by the destination node i, and TPSk, represents total packets sent by the source k. Where S, represents source and D, represents destination using Constant Bit Rate (CBR) application.

5.1 Parameters

- **Node Mobility Parameters**

The scheme is tested in a simulated environment using machine specification shown in Table 2 using NS2. Standard AODV and dynamic trusted scheme run in the presence of malicious nodes and the results obtained are presented in the section below.

The Random Waypoint Mobility (RWM) model was used to generate mobility. Parameters listed in Table 3 were used to generate mobility in NS2.

Table 2. Simulation system environment

Machine specification					
Model	CPU	CPU's speed	Memory	Memory speed (Hz)	Operating system
HPProbook 450	Intel Core i5	2.20 GHz	8.0 GB	166 MHz	Ubuntu 16.04

Table 3. Node movement and network size

Mobility model	Node movement scenarios and Network size parameters					
	Network size (node)	Malicious nodes	Topology size (m)	Transmit. range (m)	Node's speed (ms)	Pause time (seconds)	Simulation time (sec)
RWP	100	3	400 × 400	250	5–20	0–100	180

- **Parameters Specifying Traffic Patterns**

The data parameters are shown in Table 4, list all the parameters and their corresponding values used to run the simulation.

Table 4. Traffic pattern parameters 20 nodes

Conn no	Source node	Sink node	Application	Send rate	Layer 4 type	Packet size	Max pkts	Conn time
1	1	2	CBR	0.2 approx.	UDP	512	10000	2.556 approx.
2	4	5	CBR	0.2 approx.	UDP	512	10000	56.333 approx.
3	4	6	CBR	0.2 approx.	UDP	512	10000	146.9651 approx.
4	6	7	CBR	0.2 approx.	UDP	512	10000	55.634 approx.

5.2 Throughput

It is referred to as the number of packets successfully received per unit time. It is an important indicator of the performance and quality of network connection. Figure 5, shows the throughput for nodes ranging between 20–100 nodes and the comparison between trusted and standard AODV. It can be observed the due to malicious nodes introduced in the network, standard AODV having no protection has a lower throughput than the secure AODV.

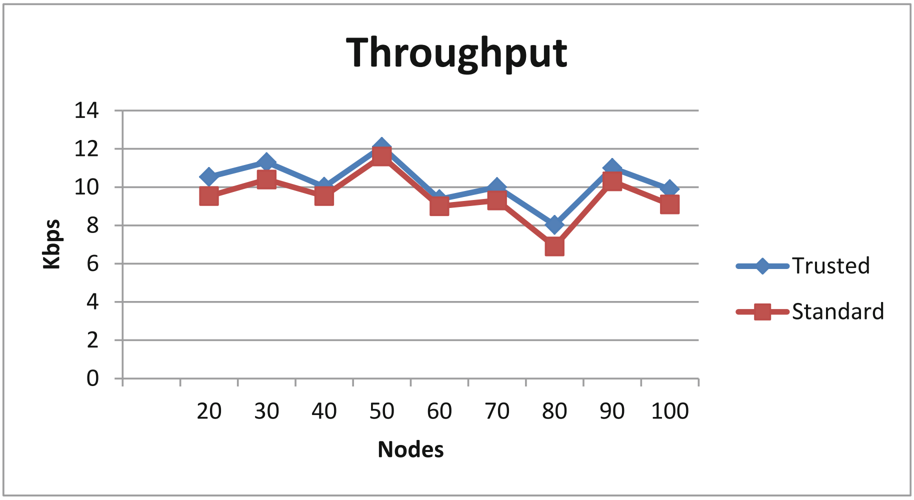

Fig. 5. Network throughput

5.3 Packet Delivery Ratio

The result for packet delivery ratio is shown in Fig. 6 below. This metric indicates the performance of the proposed trusted scheme after analysing all other performance metrics. This metric represent the ratio of the number of packets received by the destination to the number of packets sent by the destination nodes. The comparison is between standard and trusted AODV is presented in Fig. 6.

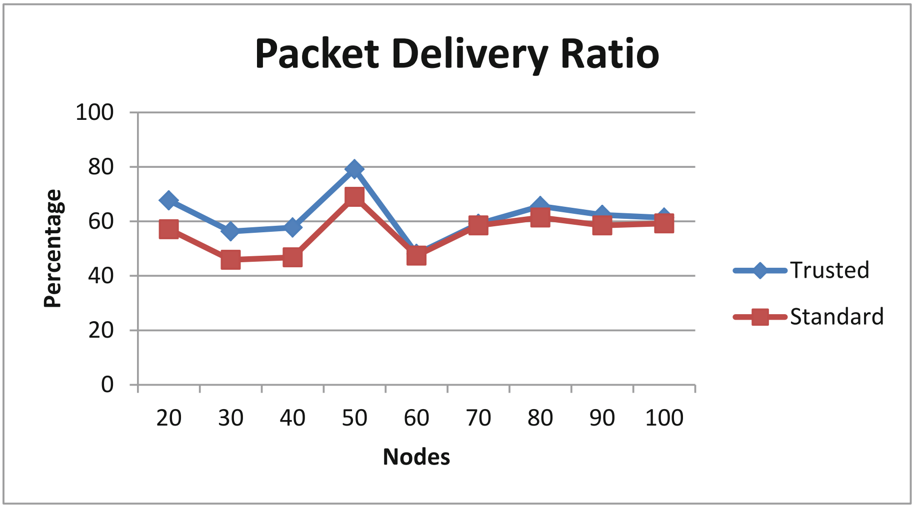

Fig. 6. Packet delivery ratio

The metrics presented to test the performance of the proposed scheme is based on data packets and do not include the control and security message i.e. the implementation of DHEC.

According to [32], there are 9 steps required to generate and exchange keys for DHEC algorithm. This means additional 9 packets are needed to the total number of packets in mutual authentication phase. The first step is peer nodes generate random number followed by generating their private and public keys. In the next step, each peer on the receipt of public key from its corresponding peer computes shared key. Therefore, there is no significant effect on the throughput when ECDH is implemented.

6 Conclusion

Determining the trust level of new nodes and allowing them to become part of the network and take part in routing and communication is still challenging issue. We proposed a novel method for authentication through trust that enabled two communicating peer nodes to prove their identity and trust level prior to exchanging data with each other. The proposed scheme provides a foundation for MANET routing protocol to implement a layer of security that enables a distributed, trusted and secure key exchange algorithm when the network initializes and ensure secure data exchange between peer nodes.

The scheme is implemented in the MANET environment with no predetermined trust therefore all nodes are treated as having no trust at all. The scheme is compatible with any MANET routing protocol and can be implemented in the network using routing protocol other than AODV.

In our proposed security scheme, we utilized common Trust based scheme for authentication and Diffie Hellman Elliptic Curve DHEC for encryption and key exchange. These schemes have some distinctive characteristic that support MANET decentralized and resource constraint environment. The trust based schemes identifies trusted and untrusted nodes while DHEC provides an efficient and secure mechanism for the distribution of key between nodes over insecure network. In our research we also propose an efficient way to support existing and new joining nodes. The scheme offers encryption of data communication using shared secret keys that are generated by the communicating nodes using DHEC algorithm. This ensures that all the nodes whether existing or new joining nodes will undergo the process of trust evaluation and authentication. The dynamic nature of the MANET makes the use of conventional security scheme such as Secret and Public Key cryptography more challenging. Therefore, the scheme proposed in this research is robust and encompasses various aspects of security. The scheme not only allows the nodes to authenticate its self but the security is implemented throughout the network and is scaled as the network grows through efficient Trust based scheme. This signifies that not only the security of individual nodes is important but the security of network as whole is of paramount importance as well and above all the security of the data communicated between is the most important of all.

References

1. Khan, I.M.S., Midi, D., Khan, M.I., Bertino, E.: Adaptive trust threshold strategy for misbehaving node detection an isolation. In: IEEE Trustcom/BigdataSE/ISPA (2015)
2. Al-Roubaiey, A., Sheltami, T., Mahmoud, A., Shakshuki, E., Moufta King Fahd, H.: AACK: Adaptive Acknowledgment intrusion detection for MANET with node detection enhancement. In: IEEE International Conference on Advanced Information Networking and Applications (2010)
3. Botkar, S., Chaudry, S.R.: An enhanced intrusion detection system using adaptive acknowledgment based algorithm. IEEE (2011)
4. Jim, L.E., Gregory, M.A.: AIS reputation mechanism in MANET. In: 28th International Telecommunication Networks and Application Conference, pp. 1–6, January 2019. https://doi.org/10.1109/atnac.2018.8615267
5. Balakrishnan, K., Deng, J., Varshney, P.K.: TWOACK: preventing selfishness in mobile AdHoc networks. IEEE Communication Society (2005)
6. Cai, R.J., Li, X.J., Chong, P.H.J.: An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. IEEE Trans. Mob. Comput. **18**, 42–55 (2019). https://doi.org/10.1109/tmc.2018.2828814

7. Buttyan, L., Hubaux, J.-P.: Enforcing service availability in mobile ad-hoc WANs. In: Proceedings of MobiHoc, August 2000
8. Zhong, S., Chen, J., Yang, Y.R.: Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In: Proceedings of INFOCOM, March–April 2003
9. Zapata, M., Asokan, N.: Securing ad hoc routing protocols. In: Proceedings of ACM Workshop on Wireless Security (WiSe), Atlanta, GA, September 2002
10. Jhaveri, R.H.: MR-AODV: a solution to mitigate blackhole and grayhole attacks in AODV based MANET. In: Third International Conference on Advanced Computing and Communication Technologies. IEEE (2012)
11. Anju, J., Sminesh, C.N.: An Improved clustering-based approach for Wormhole attack detection in MANET. In: IEEE 3rd International Conference on Eco-Friendly Computing and Communication Systems (2014)
12. Yu, M., Su, W.: A secure routing protocol against byzantine attacks for MANETs in adversarial environments. IEEE Trans. Veh. Technol. **58**(1), 449–460 (2009)
13. Rifquddin, M.R., Sukiswo, M.: Performance of AOMDV routing protocol under rushing and flooding attacks in MANET. In: Proceedings of 2015 2nd International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), Indonesia. IEEE, 16–18 October 2015
14. Hinds, A., Sotiriadis, S., Bessis, N., Antonopoulos, N.: Performance evaluation of security algorithm for AODV MANET routing protocol. In: Third International Conference on Emerging Intelligent Data and Web Technologies. IEEE (2012)
15. Juwad, M.F., Al-Raweshidy, H.S.: Experimental performance comparisons between SAODV and AODV. In: Second Asia International Conference on Modelling and Simulation. IEEE (2008)
16. Hu, Y., John, D.B., Perrig, A.: SEAD: secure efficient distance vector routing for mobile ad hoc networks. In: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002). IEEE (2002)
17. Perrig, A., Canetti, R., Tygar, J.D., Song, D.: The TESLA broadcast authentication protocol. RSA Lab. **5**(2), 2–13 (2002)
18. Hu, Y.-C., Perrig, A., Johnson, D.B.: Ariadne: a secure on-demand routing protocol for ad hoc networks. Wirel. Netw. **11**(1–2), 21–38 (2005)
19. Yi, S., Naldurg, P., Kravets, R.: Security-aware ad hoc routing for wireless networks. In: Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 299–302 (2001)
20. Carter, S., Yasinsac, A.: Secure position aided ad hoc routing. In: Proceedings of IASTED International Conference on Communication and Computer Networks (CCN 2002), pp. 329–334 (2002)
21. ARAN (A secure Routing Protocol for Ad hoc Networks) Implementation. http://signl.cs.umass.edu/arand/
22. Johnson, D., Hu, Y., Maltz, D.: The Dynamic Source Routing Protocol (DSR) for mobile ad hoc networks for IPv4. RFC 4728 (Experimental), February 2007. http://www.ietf.org/rfc/rfc4728.txt. Accessed 14 Oct 2008
23. Shakshuki, E.M., Kang, N., Sheltami, T.R.: EAACK—a secure intrusion-detection system for MANETs. IEEE Trans. Ind. Electron. **60**(3), 1089–1098 (2013)
24. Marti, S., Giuli, T., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of MobiCom, August 2000
25. Nasser, N., Chen, Y.: Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks. Reviewed at IEEE Communication Society Subject Matter Expert for Publication in the ICC 2007 Proceeding (2007)

26. Buchegger, S., Le Boudec, J.-Y.: Performance analysis of the CONFIDANT protocol: cooperation of nodes, fairness in dynamic ad-hoc networks. In: Proceedings of MobiHoc, June 2002
27. Buttyan, K.L., Hubaux, J.-P.: Enforcing service availability in mobile ad-hoc WANs. In: Proceedings of MobiHoc, August 2000
28. Sukiswo, M., Rifquddin R.: Performance of AOMDV routing protocol under rushing and flooding attacks in MANET. In: IEEE 2nd Conference of Information Technology, Computer and Electrical Engineering (ICITACEE), Indonesia, 16–18 October 2015
29. Rajesh, M., Gnanasekar, M.: Consistently neighbour detection for MANET. In: 2016 IEEE International Conference on Communication and Electronic Systems (ICCES) (2016)
30. Carter, S., Yasinsac, A.: Secure position aided ad hoc routing. In: Proceedings of IASTED International Conference on Communication and Computer Networks (CCN 2002), pp. 329–334 (2002)
31. Zhong, S., Chen, J., Yang, Y.R.: Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In: Proceedings of INFOCOM (2003)
32. Wong, Y., Ramamurthy, B., Zou, X.: The performance of elliptic curve based group Diffie-Hellman protocols for secure group communication over ad hoc networks. In: IEEE International Conference on Communication (2006)
33. Misic, J.: Traffic and energy consumption of an IEEE 802.15.4 network in the presence of authenticated ECC Diffie-Hellman ephemeral key exchange. Comput. Netw. (2008). www.elsevier.com/locate/comment
34. Gajbhiya, S., Karmakar, S., Sharma, M.: Diffie-Hellman key agreement with elliptic curve discrete logarithm problem. Int. J. Comput. Appl. **129**(12), 25–27 (2015)