Journal of Engineering Science and Technology Review 11 (1) (2018) 1 - 9

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Secured Routing Deterrent to Internal Attacks for Mobile AD HOC Networks

Menaka Sivakumar

Department of Computer Science and Information Technology, Saudi Electronic University, Abha, KSA.

Received 16 October 2017; Accepted 7 December 2017

Abstract

Security is a vital requirement for communication between mobile nodes in a hostile environment. Mobile nodes are prone to various attacks in a hostile environment. Routing is one of the crucial tasks where a malicious node can gain access to the network. This paper presents a mitigation mechanism to confront internal attacks launched by the misbehaving nodes. The nodes which launch security threats in the network after participating in the route discovery and data transmission are referred as misbehaving nodes. Such authenticated nodes misbehave either due to malicious software or get compromised. The compromised or misbehaving nodes attack on the confidentiality and authentication security services. The nodes generally gain access and become part of the network during the routing process. This works proposes a secured routing deterrent to internal attacks (SRDIA) that mitigates the internal threats launched by the compromised nodes. The proposed scheme in this paper is a defense mechanism against routing security threats for mobile ad hoc networks using ID based cryptography. In addition hash chain based security association is used for authentication and key management. This technique aims at defending from the security threats caused by compromised nodes like Byzantine attack, invisible node attack, Sleep Deprivation, location disclosure etc. In this research work an efficient authentication technique using hash chain and session key establishment is proposed. A lightweight hash algorithm "BLAKE" is used for the implementation of authentication for resource constraint devices and "PRESENT", a symmetric key encryption algorithm to secure the data exchange among nodes. The outcome of the simulation results demonstrates percentage increase of packet delivery ratio and throughput in presence of malicious nodes.

Keywords: Routing, Internal threats, Key management, Authentication, Hash Chain, Lightweight cryptography.

1. Introduction

Mobile ad hoc network is a rapidly growing technology since it is fast and easy to setup without the need for any infrastructure. MANET is a self organized and rapidly deployed network by node's cooperation to communicate [1]. Every node is autonomous in behavior that is it may act as a host or a router to forward message to the other nodes to enable communication. The accessibility to the information and services regardless of geographic position, flexibility of fast establishment of the network, scalable to accommodate any number of users are some the advantages of a mobile ad hoc network. A MANET also possesses various challenges in terms of resource constraints and security issues. The wireless transmitter and receiver enable communication among the nodes in its wireless vicinity. The nodes which are not in the wireless vicinity establish multihop communication governed by a set of rules (routing protocol) as depicted in figure 1.

This process of establishing multihop connectivity is termed as routing. Routing is a key feature of the network that enables messages to pass from one node to another and eventually reach the target node. Each intermediary node performs routing by passing along the message to the next system thence is considered as one of the crucial tasks where a malicious node can gain access into the network. The routing challenge in such an environment is to protect the network from the various types of routing attacks. The absence of central infrastructure, dynamic topology, resource constrains and wireless channel enforces security challenges for routing in mobile ad hoc network. Albeit the MANET posses beneficial features it is still assailable to security threats are listed below as given by [2]

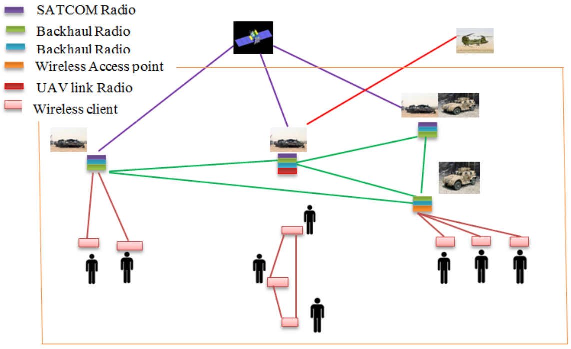

Fig. 1. View of Mobile Ad Hoc Network Setup in Battlefield

i) Lack of Centralized management: Ad hoc networks are self organized collection of nodes and hence centralized monitoring of the network activities are not present. This makes the detection of attacker a difficult task which requires separate security procedures embedded with the nodes.

ii) Absence of clear of line of defense: The nodes operate in a peregrine environment where they are allowed to join and leave the wireless network. Hence when any adversary

*E-mail address: smenaka76@gmail.com

doi:10.25103/jestr.111.01

perforates into the radio range the resources of the network will be accessible.

iii) Cooperativeness: The communication between the nodes is enabled through cooperativeness of the intermediate nodes to forward the data [3]. The routing algorithm execute with the assumption that the nodes are cooperative and non-malicious. Routing is a task where the malicious attacker could gain access and disrupt the network.

iv) Dynamic Topology: Any nodes may join or leave the network due the mobility nature of the nodes that leads to the frequent changes in the network topology and the connectivity among the nodes [1]. The unpredictable frequent changes in topology effectuate the complexity of the routing algorithms.

v) Resource constraints: The restricted availability of the power capacity, computational capacity, memory and bandwidth inflict the security and reliability of the communication between the nodes. This fact of limited the resources also increases the complexity of routing.

Despite the benefits of ad hoc networking, the characteristics of the wireless communication medium and the mobility of nodes create a complex, unpredictable and challenging environment [4]. Routing is one of the mandatory tasks to commune the nodes in an ad hoc network that operate in adversarial environments in which security is a more challenging issue. An efficient routing protocol must converge quickly and should keep track of the changes in the topology which could be achieved only if proper cooperativeness exists among the nodes. Since the routing protocols function in a hostile environment it is susceptible to various security threats. The security attack can be raised by nodes that do not possess the credentials to participate in the protocol termed as external attacks. Various researchers have proposed secured routing protocols addressing the external attacks using encryption, authentication and integrity mechanisms. Nodes that possess all the credentials to gain access to the network and take part in the routing get compromised due to the software vulnerabilities and disrupt the network performance. Such attacks caused by the authenticated nodes are known as internal attacks. The malicious nodes that induce internal attacks are already a part of the network, which makes it difficult to detect such attacks **[2].** Byzantine attack invisible node attack, location disclosure attack, sleeps deprivation and selfish node attacks are some of the severe internal routing attacks currently in the research findings.

This study proposes a novel mechanism to mitigate the impact of such internal routing attacks using peer to peer security association for key management, identity based cryptography for authentication. The proposed design of the secured routing algorithm is simulated in NS3 for the study of its efficiency. The rest of the paper is organized as section 2 discussing the various internal routing attacks, section 3 details the research findings of the solutions defending the attacks and the various literature of the authentication and key management techniques are discussed in section 4. The proposed secured routing mechanism is discussed in detail in section5 supporting with the simulation results in section 6 and concluding remarks in section 7.

2. Related work

2.1 Routing attacks

The transmission of data between the nodes not in their vicinity is achieved with the cooperation of the intermediate nodes forwarding the data packets to the destination node. Hence every node in a mobile ad hoc network has the functionality of a router to make routing decisions to forward the data packets they receive. As mentioned in [1], routing protocols reckon active cooperation of the nodes to establish and operate the network. The dynamic, distributed infrastructure less nature and lack of centralized authority makes the ad hoc network vulnerable to various kinds of attacks. The open wireless channel provides accessibility to all type of nodes that are obnoxious to malicious attackers. The behavior and impact of the attacker classifies the routing attacks as active and passive attacks. The source of the attacks categorizes as external and internal attacks.

2.2 Active attacks vs Passive attacks

Active attacks aim to obstruct the operation of targeted networks while passive attacks are plunged to extract the valuable information about the target networks. Eavesdropping and traffic analysis attacks fall in the category of passive attacks that violate the confidentiality paradigm. Injecting packets to invalid destinations, deleting packets, modifying the contents of packets, impersonating other nodes, message modifications, message replays, message fabrications and denial of service are examples of active attacks that violates availability, integrity, authentication and non-repudiation paradigms.

2.3. External vs Internal attacks

The activities of adversaries that are not authorized to take part in the routing operations set in motion the external attacks. These types of attackers focus to cause network congestion, denying access to specific network function or to disrupt the whole network operations. Examples of attacks that are constituted by such unauthorized nodes include bogus packet injection, denial of service, and impersonation. Such type of external attacks initiates the most well known attacks like wormhole attack, black hole attack, flooding and rushing attacks. In contrary to external attacks, [5] the internal attacks are launched by the nodes that are authorized to participate in the network operations and then get compromised to disrupt the target network. Byzantine attack, route salvaging, invisible node attacks are examples of internal attacks that are shot from both compromise and misbehaving nodes. The discern between normal network failure and misbehavior activities in the ad hoc network is a hard task that makes the detection of an internal attack more difficult than detecting the external attack.

2.3.1. Byzantine attack

This is one of the most conspicuous internal attacks according to [6]. An authorized node colludes with group of nodes within the network creating routing loops, forwarding the packets through non optimal path disrupting and degrading the routing services.

2.3.2. Route salvaging attack

The attacks launched by greedy internal nodes which retransmit **[7]** the packets through an alternate path without receiving the route error message. The impact of the attack results in draining off the resources in the intermediate and destination nodes and hence categorized as resource consumption attacks.

2.3.3. Invisible node attack

The Invisible node attack is a different and a unique form of attack as defined by [8]. It is described as a node that actively participates in the route discovery without revealing its identity that is an attack based on identity functionality. Table 1 summarizes the various internal routing attacks.

Table 1. Internal Routing Attacks

Threat	Caused By	Type of disruption: RC/RD
Byzantine Attack	Colluding compromised node, routing loops	RD: Route disruption
Route Salvaging	Redirect data packet in a different path.	RD: Route Disruption
Invisible Node	Take part in route without revealing its identity	RD & RC
Selfish Node Misbehaviour	Take part in the routing and doesn't forward data packets / drops data packets	RC: Resource Consumption

Various researches have proposed the secured routing protocols that address only a subset of the above attacks mentioned. Most of the work in the literature focus on proposing an efficient authentication mechanism to prevent the malicious nodes gaining access to the network. The mitigation of the effect launched by internal malicious nodes can be enforced with more suitable and efficient authentication techniques. Key management schemes play a major role in facilitating an efficient authentication of an entity that adds to the complexity. Various proposed solutions to defend the internal attacks that exist in the literature is briefed in the following section.

2.4 Literature

An On-Demand Secure Byzantine Routing protocol (ODSBR) was the initial algorithm proposed by **[4]** that detects an abnormal behavior of an authenticated node and deflect its upshot. It uses the public key based authentication for route discovery and symmetric key techniques for the other phases in routing. This algorithm uses the reliability metric represented by the link weight to select the path. The link weight information is obtained from the past history profile. The demerit of the ODSBR could be summarized as it is basically an intrusion detection approach, and the metric to select the path is based on the history which would not be the same always. Dynamic updating of link weight information adds to the additional complexity of the technique. Moreover ODSBR algorithm doesn't address the resource consumption attacks launched by the compromised nodes as given by **[6]**

In **[10]** presented a technique that detects internal attack through redundancy of route and routing messages in the route discovery phase. They have proposed pair wise secret between source and destination to protect the route discovery message and public key cryptosystems to validate the intermediate nodes along the path. An optimal routing algorithm was devised using node's trustworthiness based on the performance as the routing metric. Though this work has demonstrated a better performance trust based techniques incurs computational expenses to compute the trust values and the in fact information is not secure [11] and stable.

As proposed by author in [12], implemented the algorithm to identify and prevent the malicious nodes using a semantic security mechanism. The technique involves a two way communication that generates the hash code and flow conservation to identify the threshold value for packet dropping to detect the misbehavior of the nodes. The main drawback of the proposal is that the detection process is done as an independent task that should be performed periodically to detect the compromising nodes. Additional task exclusively executed incurs overhead in terms of computational capacity specifically in resource constrained devices.

A hybrid security and trust base routing scheme is described in **[6]** to detect byzantine and black hole attacks. The mechanism is based on secure auto configuration and enhances secured public key distribution for authentication of the nodes to join the network. Message integrity is achieved by keyed Hash MAC over a shared secret key. This algorithm provides a tradeoff between security and energy consumptions. Key management scheme incurs computational overhead and improving the QoS in terms of efficiency of the protocol are the future improvisation of the proposal.

In **[9]** the authors have proposed a concept of intrusion information that consists of profile of path of packet flow known as profile based protection scheme. The captured information by the module analyses the difference in profile status in normal and presence of worm node. The profile contains the details of the attacker node like node number, port number, time of intrusion and type of attack. These parameters are acquired by passing the probing packets in the network. The present scheme is self organized, distributed and localized procedure but still suffers from the drawback that it incurs traffic overhead due to exchange of probing information.

2.5. Need for current work and contributions

Most of the techniques involve efficient authentication mechanisms to verify a node that join the network. The literature study concludes that the existing work to extenuate from the attacks of compromised nodes after joining the network is only based on detection of the presence of attack. In addition the intrusion detection or prevention scheme performs with the behavior profile of the node which would not be similar for all types of scenarios. Thence a more sophisticated and computationally efficient authentication and key exchange mechanism has to excogitated to detect the probability of presence of malicious node. In this research work an efficient authentication technique using hash chain and session key establishment is proposed. According to authors of [16], There is a strong need to employ lightweight cryptographic primitives for many security applications because of the tight cost and constrained resource requirement of mobility based networks that comprises of mobile devices as network nodes. Hence a lightweight hash algorithm "BLAKE" is used for the implementation of authentication for resource constraint devices and "PRESENT", a symmetric key encryption algorithm to secure the data exchanges among nodes. The following section details the secured routing scheme proposed.

3. Proposed hash chain based authentication

The proposed model comprises of three phases as given in the figure 2. In our proposed scheme of establishing secured route in a mobile ad hoc network is done in two levels of authentication of the nodes. The first level of legitimacy of the node is achieved by establishing peer-to-peer security associations **[13]**. Security associations facilitate to authenticate the intermediate nodes in the route. The second level of genuineness is confirmed by verification of hash values generated in the hash chain.

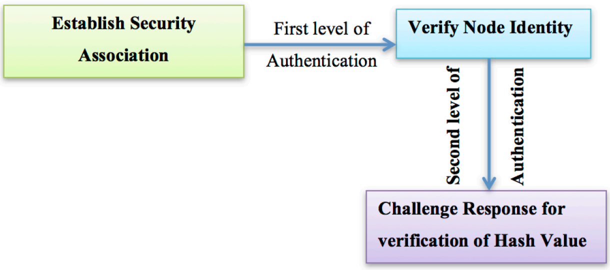
Establish Security Association
First level of Authentication
Verify Node Identity
Second level of Authentication
Challenge Response for verification of Hash Value

Fig. 2. Hash Chain Based authentication Scheme

The system model comprises three phases viz.

Phase 1: Establishment of security association
Phase 2: Node verification
Phase 3: Session key exchange

3.1. Security association

Security association is a secured channel established between two entities in a network to provide a secured communication. In an ad hoc self organizing network, the node with a single shared key will not be efficient to use for communication due to the security issues raised by the mobility nature of the nodes. Hence, it is proposed to have a Node's ID based key exchange for establishing the security association. The node's ID comprises of the IP address and MAC address to minimize the IP spoofing attack. When a node joins a network it initially establishes the direct security association with its neighbouring nodes that are within its vicinity. A Security association is established by exchanging the node's ID, MANET ID and its public key which is given below.

$$S.A = [ID_N \,||\, K_N \,||M_{ID} \,||\, S_M]$$

ID_N: ID consists of Node MAC address and network interface derived from its IP address
K_N: Public key of the node derived from node's ID
M_{ID}: Network's ID
S_M: Shared MANET key

The public key of the node is a self generated key pair that eliminates the dependency of a third party or public key infrastructure to authenticate a node. The node already existing in the network on receiving the security association parameters decrypts the information using the MANET key and verifies the public key of the node for the first level of authentication. Since the public keys are self generating based on the node's identities, the public key is verified by the receiving node and the security association will be established, or else it will be denied. The public and private keys are self generating key pair using bilinear pairing as illustrated in the Figure 3.

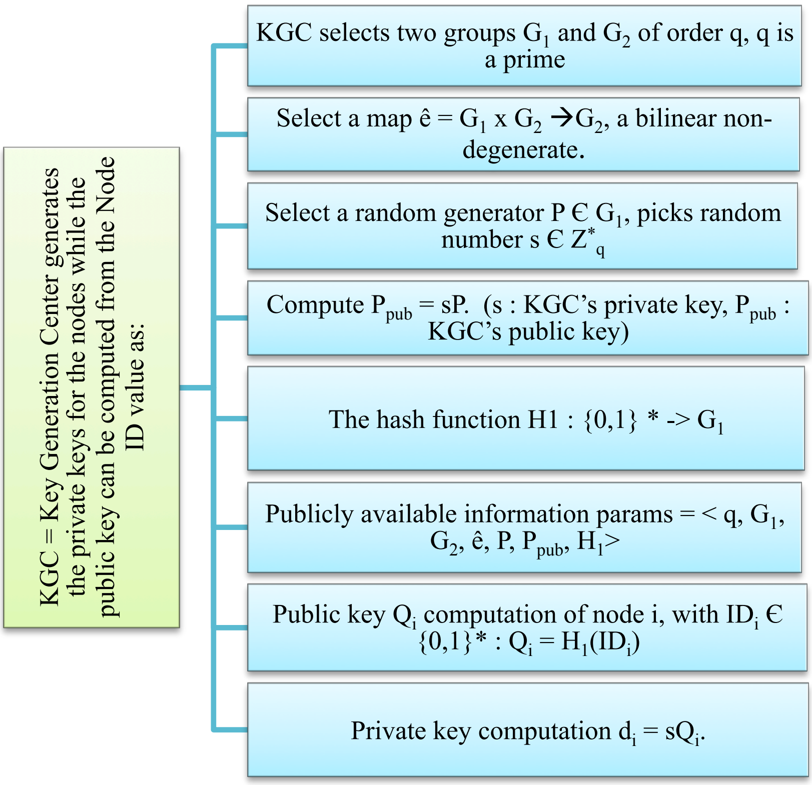
KGC = Key Generation Center generates the private keys for the nodes while the public key can be computed from the Node ID value as:
KGC selects two groups G_1 and G_2 of order q, q is a prime
Select a map ê = G_1 x G_2 → G_2, a bilinear non-degenerate.
Select a random generator P Є G_1, picks random number s Є Z^*_q
Compute P_{pub} = sP. (s : KGC's private key, P_{pub} : KGC's public key)
The hash function H1 : {0,1} * -> G_1
Publicly available information params = < q, G_1, G_2, ê, P, P_{pub}, H_1>
Public key Q_i computation of node i, with ID_i Є {0,1}* : $Q_i = H_1(ID_i)$
Private key computation $d_i = sQ_i$.

Fig. 3. Self Generation of Key Pair Using Bilinear Pairing

3.2. Secured routing

The secured routing in this proposed model is implemented by using hash chain. As in the case of on-demand the source node initiates routing the route discovery by broadcasting the RREQ packet to its neighbour nodes. The communication link between the single hop nodes are already secured; as the security association is established between the neighbouring nodes and the representation is provided in the Figure 4.

The source node ‘S’ broadcast RREQ packet to its next hop nodes ‘N1’ and ‘N2’ via directs security association. Similarly, the corresponding nodes forward the RREQ packet via direct secured channel to their next hop node. This process continues until the destination node is reached. The source node generates the initial seed value ‘k’ and adds its hash value $H_0(k)$ in the RREQ packet forwarded for route discovery. The next hop node that receives the RREQ from ‘S’ computes the hash value of $H_0(k)$ as $H_1(H_0(k))$ and forward the same to nodes ‘N3’ and ‘N4’. In a similar fashion the chain of hash values are computed at the intermediate nodes and reach the destination node. If the route is composed of ‘n’ intermediate nodes, the destination node receives $H_{n-1}(k)$. Since, the intermediate nodes communicate only through security association established initially; the hop to hop authentication of the route is ensured. The processing of the RREQ packet at the intermediate node is shown in the Figure 5.

In this route discovery scheme, the route salvaging is eliminated where the compromised node cannot inform a false route to the source. The next phase is the process of the target node replying by unicasting a RREP packet to the source. This phase is piggybacked with the process of establishing the indirect security association with the source via the intermediate nodes (D→N7→N4→N1→S) as shown in the Figure 6.

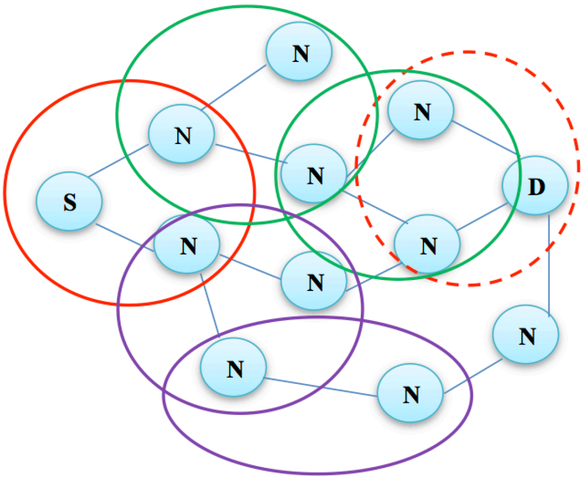

Fig. 4. Illustration of Route Discovery

A common session key for communication between the source and destination is also generated in this phase. The session key generated is used to encrypt the data packet such that the intermediate nodes cannot gain access to the data exchanged between nodes ‘S’ and ‘D’.

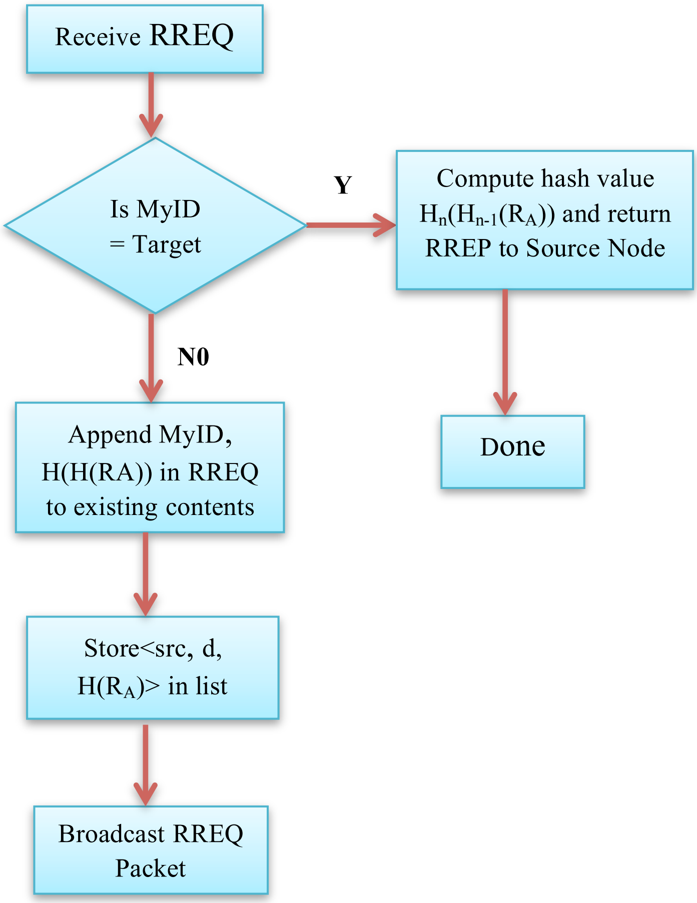
Receive RREQ
Is MyID = Target
Y
Compute hash value $H_n(H_{n-1}(R_A))$ and return RREP to Source Node
N0
Done
Append MyID, H(H(RA)) in RREQ to existing contents
Store<src, d, $H(R_A)$> in list
Broadcast RREQ Packet

Fig. 5. Route Discovery Process at the Intermediate Node

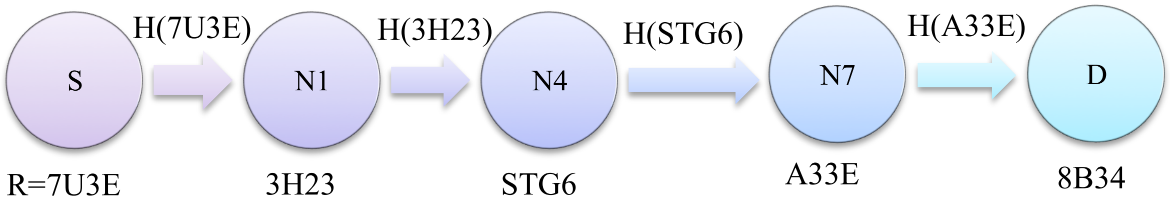

Fig. 6. Hash Chain Establishment in Route Discovery

3.3 Session key establishment

The verification of the destination node and session key generation is shown in the Figure 7 below.

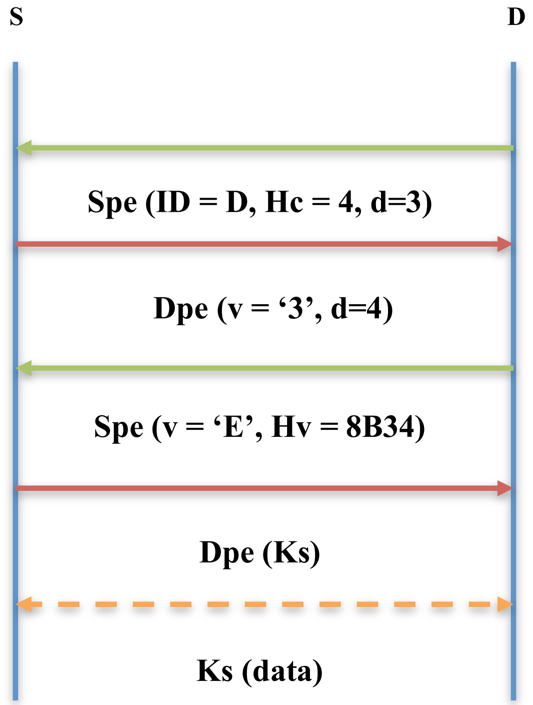

Fig. 7. Session Key Establishment

The source and destination node have now established the session key through the challenge response scheme. The node 'S' acts as the challenger while node 'D' is the challengee. The destination node generates the public key from the identity details of the source. Then the challenge communicates its ID information, hop count (Hc), and asks for a digit at some location'd' of the next hash value. All the parameters are encrypted by the challenger's (source) public key (derived from id details of the node). The challenger decrypts the information acquired with its private key and responds with the correct value and asks for the digit at some location of previous hash value. Again, this information is encrypted with the challengee's (destination node D) public key. At the destination, it is decrypted with its private key and responds with corrected digit and next hash value. The challenger verifies the authenticity of the challengee (node D) shares the session key generated to the destination. The further communication is processed by encrypting/decrypting with the session key. The hash values of the destination node for different number of hop counts will be maintained along with the route in the path cache. When the route is changed from the current route to a different route, the same key establishment procedure is executed to verify the destination.

3.4 Security analysis

This proposed model of secured routing using peer to peer security association based on hash chain eliminate the access to the external malicious nodes [14]. Internal routing attacks like invisible node attack is addressed by this proposed model as the security association is established by exchanging their ID as a part of the information. The intermediate nodes cannot modify the information exchanged for node verification as it is encrypted by the public key of the recipient and hence the probability of route falsification error is also considerably reduced. In a similar fashion, the communicated data is also encrypted with a shared secret session key which is also immune to any type of passive attack by the compromised nodes [15]. In this present routing scheme, the malicious or misbehaving nodes impact is favourably reduced and hence prevented. The strength of the security features of routing scheme is studied under NS3 simulation for further analysis and Table 2 gives the security features of the technique.

Table 2. Security Features of SRDIA

Attack	**Technique to defend / detect**
Invisible Node attack	ID based authentication
Byzantine Attack	Security Association
Sleep Deprivation	Hash Chain
Eavesdropping	Session Key

4. Simulation and results

Simulations were conducted in NS-3 to analyze the performance of the proposed secured routing scheme. The performance of the proposed authentication and key establishment techniques is investigated by varying the number of malicious node's present in the network. The evaluation metrics like the packet delivery ratio and throughput in the presence of malicious nodes are derived and compared with the performance of normal DSR and ODSBR protocols. Hashing is implemented using BLAKE512 and the symmetric key encryption is implemented using PRESENT algorithm. The above mentioned algorithms are lightweight cryptographic techniques that reduce the initial route acquisition time incurred in authentication and verification of the node's legitimacy. The following section describes the simulation set up parameters and highlights the results obtained from the simulation.

4.1. Simulation Design

The simulation set up of the network is detailed in the Table 3. The network area is 1500 x 1500 square meters with a bandwidth of 2MHz in a two ray propagation model controlled by random by a maximum of 100 nodes. The mobility pattern of the nodes is ascertained by random way mobility model with a constant bit rate traffic of generating 4 packets per second of 512 bytes size. The simulation is run for 10 iterations, each for 1000 seconds to acquire the accuracy of the evaluation. The selective packet drop attack and flooding attack in the adversary models used to analyze the secured routing scheme.

Table 3. Simulation Setup Parameters

Parameters	Values
Number of Nodes	100
Topology area	1500 x1500 Sq. m
Traffic type	CBR (Constant Bit Ratio)
Mobility Model	Radom Way Point model
Simulation Time	1000 secs
Application Data Payload	512 bytes / packet
No: of packets	4 packets/second
Cache size	15 routes

4.2. Discussions

The simulation is run for different pause time as 0, 5, 10, 15 and 20 ms and the nodes velocity range as 5m/s to 20 m/s. The performance analysis of the proposed routing scheme SRDIA (Secured Routing Deterrent to Internal Attacks) and ODSBR (On Demand Secured Byzantine Resilient) protocol is represented in the Figures 8 to 10. The behavior of the normal DSR protocol in the presence of adversaries was also analyzed. The packet delivery ratio is defined as the fraction of data packets received to the data packets generated at the source, which is expressed as:

$PDR[\%] = \frac{\sum_{i}^{n} received}{\sum_{1}^{m} sent}$ x 100, where

n = number of packets received
m = number of packets sent

From the simulation results, a gradually decreasing linear trend was noted for all the three routing protocols which are shown in Figure 8. It can be derived that a significant difference exists in the diminution of packet delivery ratio in the case of normal DSR and SRDIA.

A linear empirical relationship was computed for 10 simulation runs varying the pause time and the mobility speed of the nodes. An acceptable regression coefficient above 0.98 was obtained for average packet delivery ratios (PDR) in the presence of adversary nodes ('a') represented in the equations 1, 2, 3.

i) DSR:
$$PDR = -3.7571a + 79.952 \quad (1)$$

ii) ODSBR :
$$PDR = -2.4143a + 81.238 \quad (2)$$

iii) SRDIA:
$$PDR = -1.7571a + 92.952 \quad (3)$$

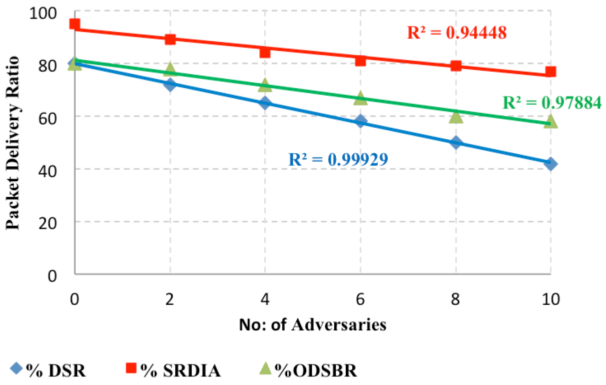

Fig. 8. Packet Delivery Ratio in Presence of Adversaries

When the number of adversary nodes 'a' is substituted as 10 in the above equations the packet delivery ratio is obtained as 42.381, 57.095 and 74.381 for DSR, ODSBR and SRDI respectively. It is clear that the average PDR for proposed SRDIA was nearly 30% higher than the existing DSR and ODSBR protocols in the presence of malicious nodes. It is also observed that the decrease of PDR in SRDIA is only 18% with respect to initial state while the normal DSR exhibits a sharp declination of 37% with the increase in the number of adversaries in the network.

Throughput is defined as the total number of data packets delivered during the total simulation time and it is given by:

Throughput = N / T

Where, 'N' - number of bits received successfully at the destination and 'T'- total simulation time.

About 24% higher throughput is gained with the proposed technique compared with the throughput performance of ODSBR in the presence of malicious nodes. It is also discernible from the trend line given in Figure 9 that there is a sharp declension in throughput of ODSBR and DSR compared to the decrease in SRDIA with an increase in the number of adversary nodes.

A regression coefficient of above 0.97 is obtained for the empirical equation that is derived from the simulation runs for varying pause time and the mobility speed of the nodes for average throughput. A non-linear empirical equation was found to best fit for the given points of the throughput achieved by SRDIA, DSR and ODSBR techniques in the presence of adversary nodes as given by the Equations 4, 5 and 6 below.

i) DSR:
$$Th= -0.1487a^{3} + 2.7023a^{2} - 19.308a + 91.292 \quad (4)$$

ii) ODSBR:
$$Th = -0.0853a^{3} + 1.5955a^{2} - 13.676a + 89.87 \quad (5)$$

iii) SRDIA :

$$Th = 0.0019a^3 + 0.1704a^2 - 5.7019a + 89.653 \quad (6)$$

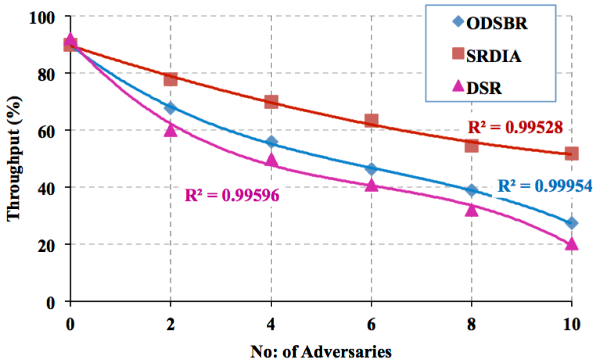

Fig. 9. Throughput in Presence of Adversaries

In the above equations, when the value for number of adversaries (a) is substituted as 10, the throughput obtained was 19.742, 27.143 and 51.574 for DSR, ODSBR and SRDIA respectively. The throughput value clearly indicates that on an average 55% higher throughput is observed in SRDIA when compared with the DSR and ODSBR techniques. Reliable predictions of the output were observed from the above equations which conform to the simulation results.

As mentioned earlier in this study, various attacks were induced to observe the impact of the proposed defensive technique against adversaries. One such attack is a selective drop attack that selectively drops the data packets after taking part in the route. The simulation results are plotted in the trend line as shown in Figure 10. A non-linear increase in the rate of dropped data packets is exhibited by DSR and ODSBR while a gradual increase is observed in SRDIA. The security association established initially while joining the network provides the data forwarding security and hence sustains the effect of the attack before any disruption to the communication or the network. It is observed that 65% lesser percentage of data packets dropped due to the misbehaviour of the malicious nodes in SRDIA than the packet drop percentage in DSR and ODSBR.

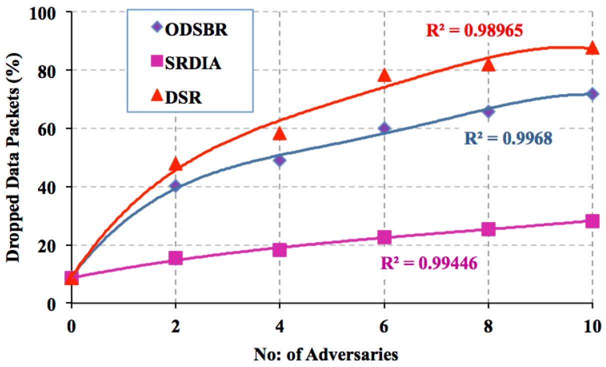

Fig. 10. Dropped Data Packets in the Presence of Adversaries

A non-linear trend line was found to best fit the given simulation points and also exhibited an increase in percentage of packet drop relative to the increase in the adversary nodes. It is also observed that the rate of increase is gradual in the case of proposed technique (SRDIA) when compared to the DSR and ODSBR.

i) DSR:

$$P_{drop} = -0.0255a^4 + 0.5993a^3 - 5.3376a^2 + 26.81a + 9.024 \quad (7)$$

ii) ODSBR:

$$P_{drop} = -0.0254a^4 + 0.6149a^3 - 5.341a^2 + 23.6a + 8.9821 \quad (8)$$

iii) SRDIA:

$$P_{drop} = 0.0116a^3 - 0.2679a^2 + 3.4808a + 8.6994 \quad (9)$$

When the number of adversaries ‘a’ is substituted as 10 nodes in the above equations 7 to 9 exhibited 87.6%, 75.7% and 28.4 % of packet drop in DSR, ODSBR and SRDIA respectively. It is apparent from the points predicted for the above trendline that, SRDIA yields on an average of 65% lesser packet drop than ODSBR and DSR respectively.

The above results corroborate that the proposed authentication and key management scheme is more efficient to palliate the impact of the malicious nodes.

5. Conclusions

The present study proposed an ameliorated authentication and key management scheme for secured routing deterrent to internal attacks in self organizing networks. There are various salient features realised from the projected technique. This technique provides two level of authentication of intermediate hop nodes through security association and hash chain values. The hash chain is developed along the path, the route salvaging threat is avoided. The challenge-response scheme to establish a session key combats the man-in-middle attack because, the refreshed values were considered invalid during validation. Every pair of nodes exerts a session key to accomplish the confidentiality of the data packets that prevents eavesdropping attack. The survival time of the session key can be decided by the life time of the route, which is based on the cross layer approach. Use of lightweight cryptography for resource constrained devices facilitates to compromise with the initial authentication and key establishment delay induced in route acquisition. It is also evident from the results that the degradation of the performance factors like the end to end delay and throughput being lesser than the ODSBR and basic DSR protocols. The performance of the algorithm was explored by simulating in NS-3 in the presence of adversary nodes. Although this showcases improved performance, it incurs an initial route acquisition delay due to the verification and session key establishment processes which is compensated by application of lightweight cryptography techniques for hashing and encrypting. Detecting the presence of malicious nodes and the revoking of the node’s authorization is the extension of the proposed technique.

References

1. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, “A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks”, Journal of Computing, Volume 3, Issue 1, January 2011
2. Priyanka Goyal, Sahil Batra, Ajit Singh, “A Literature Review of Security Attack in Mobile Ad-hoc Networks”, International Journal of Computer Applications (0975 – 8887), Volume 9– No.12, November 2010
3. Aarti, Dr. S. S. Tyagi, “Study of MANET: Characteristics, Challenges, Application and Security Attacks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013
4. Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru, Herbert Rubens, “ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks”, ACM Transactions on Information Systems Security (TISSEC), vol. 10. no. 4, January 2008.
5. S. A. Razak, S. M. Furnell, P. J. Brooke, “Attacks against Mobile Ad Hoc Networks Routing Protocols”, Proceedings of the 5th annual postgraduate symposium on the convergence of telecommunications, networking and broadcasting (PgNeT), Liverpool, June 28-29, 2004. PgNeT, pp.147-152.
6. Jayashree Padmanabhan, Tamil Selvan Raman Subramaniam, Kumaresh Prakasam and Vigneswaran Ponpandiyan, “A Secure Routing Protocol to combat Byzantine and Black Hole Attacks for MANETs”, First International Conference on Advances in Computing and Communications (ACC 2011)
7. Abhiskek Ranjan, Venu Madhav Kuthadi, Rajalakshmi Selvaraj, and Tshilidzi Marwala, “Detection and Avoidance of Routing Attack in Mobile Ad-hoc Network using Intelligent Node”, International Conference on Information Technology and Computer Systems Engineering (ITCSE'2013) Nov. 27-28, 2013 Johannesburg (South Africa)
8. Todd R. Andel, Alec Yasinsac, “The Invisible Node Attack Revisited”, n Proceedings of IEEE Southeast Con2007, Richmond, VA, Mar 22-25, 2007, pp. 686-691.
9. Varsha Shrivastava, Prof. Pradeep Mishra, “A Novel Protection Scheme against Byzantine Attack in Mobile Adhoc Network”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 4, April 2014
10. Ming Yu, Mengchu Zhou,and Wei Su, “A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments”, IEEE Transactions On Vehicular Technology, Vol. 58, NO. 1, January 2009
11. Jared Cordasco1 Susanne Wetzel, “Cryptographic Versus Trust-based Methods for MANET Routing Security”, Electronic Notes in Theoretical Computer Science 197 (2008) 131–140
12. G.S. Mamatha and Dr. S. C. Sharma, “A Highly Secured Approach against Attacks in MANETS”, International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010
13. Vikas Madan, Ashwani Kush"“Review of Hashing as Security Tool in Wireless Ad Hoc Networks, www.docstoc.com/ Business/ Articles
14. Thomas Page, “The application of hash chains and hash structures to cryptography”, A thesis submitted for the degree of Doctor of Philosophy, Royal Holloway, University of London July 27, 2009
15. Zhang Yi, Zhu Lina And Feng Li, “Key Management And Authentication In Ad Hoc Network Based On Mobile Agent” Journal Of Networks, Vol. 4, No. 6, August 2009
16. Manjulata, Adarsh Kumar, "Survey on Lightweight Primitives and Protocols for RFID in Wireless Sensor Networks", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 6, No. 1, April 2014