Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 13, Number 2 (2017), pp. 431-452

http://www.ripublication.com

Mitigation of Wormhole Attack using SOA in MANET

Vimal Kumar and Rakesh Kumar

Madan Mohan Malaviya University of Technology, India

Abstract

Development of security protocol in mobile ad hoc network (MANET) is a very challenging task. It is vulnerable to various security attacks due to dynamic topology, absence of centralized authority, limited resources etc. One of the prominent security threats that hamper the confidentiality and integrity of message being sent is called wormhole attack. A wormhole attacker creates a tunnel like structure comprising two or more malicious nodes and replay packets to each other in the network. There are some approaches (SAODV, ARIDAN) are used to minimize wormhole attack effect on the network. These schemes do not provide some important characteristics, viz., interoperability, flexibility, interoperability, confidentiality and secrecy of packets. In this article, a service oriented architecture (SOA) based signature scheme has been proposed to mitigate wormhole attack. SOA is a type of middleware that supports application development and communication through various services deployed at every node constituting the network. It has three fundamental modules, viz., service broker, service provider and service consumer which work collectively to provide functionality as requested by a mobile node. These services are provided according to need of applications running on mobile devices such as laptop, PDA. Simulation results conducted in network simulator (ns-2). It shows that wormhole attack is mitigated successfully and it outperforms over existing schemes in terms of packet delivery ratio, end-to-end delay and throughput. Our SOA based signature scheme provides various benefits such as interoperability, flexibility, heterogeneity, coupling, platform-independence, scalability, reusability and

some security goals such as authentication, non-repudiation and integrity. It also outperforms over existing schemes in terms of packet delivery ratio, end-to-end delay and throughput.

Keywords: MANET, Wormhole attack, SOA, Bilinear pairing, SAODV.

INTRODUCTION

Devices on any network can exchange information either through a wired or wireless medium. Unlike wired medium, nodes in wireless network communicate directly if source and destination lie in each other's radio range else every node cooperate to provide multi-hop communication so such network have nodes that can behave as a router as well. Wireless network are of two types, fixed and ad hoc network. In fixed network communication is done through the fixed base station, whereas in MANET [1] nodes can freely move so there is no fixed topology and neither is any fixed governing body. Such structure removes the drawback of having a single node bottleneck on one hand, but on another there are several security threats to such network. As routing in such network depend upon co-ordinate effort of every node so attacker can easily launch an attack by compromising any node hence providing security to MANET is call of time as such network are beneficial to various real- time application like locating soldiers in the military troop on any surprise attack.

Classification of security attacks*:* It can be classified in two broad categories such as passive and active attack.

Passive attack: There is no loss or modification of data as attackers aim to obtain information like number of packets sent, the frequency of communication. Eavesdropping is a kind of passive attack.

Active attack: In this attack, attacker modifies the content of a message like fabrication and packet dropping. Wormhole is a kind of this attack.

Wormhole attack: Wormhole attack [2] is a type of active attack. It forms a tunnel like passage between two or more malicious nodes and replay packets between them. Such attack can misguide non- adjacent nodes by making them believe that they are present in each-other's proximities which eventually disrupts the working of routing protocol and brings the network down.

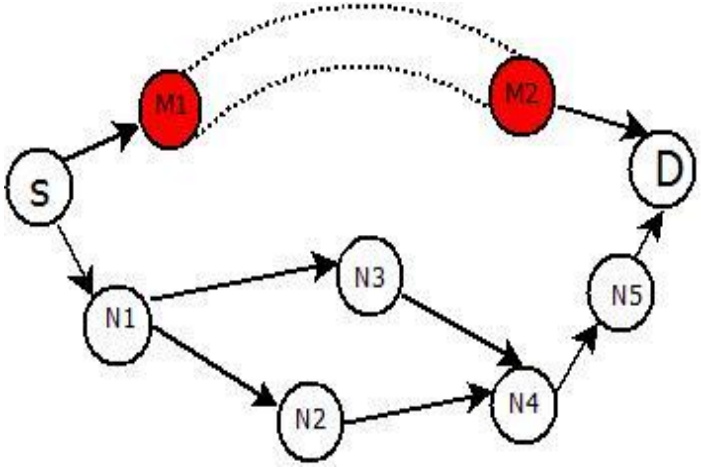

Figure 1: Wormhole attack

In Figure 1 malicious node M1 and M2 trick source node S into believing that there is shortest route S-M1-M2-D with less hop count than S-N1-N3-N4-N5-D which is valid and actual path. Depending upon the types of tunnelling and attacker, location of victim node, there are different types of wormhole attack [3-5]:

- **Open, half open and close wormhole:** When both malicious nodes are visible in the source and destination nodes, it is called an open wormhole, when one of the malicious nodes would be visible, it will be called half close and when both malicious nodes are not visible it is called close wormhole attack.
- **Encapsulation based wormhole*:*** When an attack is launched by encapsulating the packet at one end of the tunnel and decoding at the other end.
- **Out-of-band channel wormhole:** When both malicious nodes are directly connected using channel of high bandwidth.
- **High power transmission wormhole:** When both malicious nodes have capacity of high power transmission, an attacker can use this type of attack
- **Protocol deviation based wormhole:** In order to attack, the attacker causes a deviation in routing method that is being used which can result in the discarding of genuine packet.
- **Threshold, all pass and all drop based wormhole:** If the classification of wormhole attack is based on the type of data that tunnel can carry, a wormhole can be either threshold based where only packet having size smaller than

threshold can be passed or all pass based where all packets get passed or all drop based where every packet get dropped.

Taxonomy of wormhole attack: Taxonomy of wormhole attack is divided into three broad categories, which is shown in Figure 2.

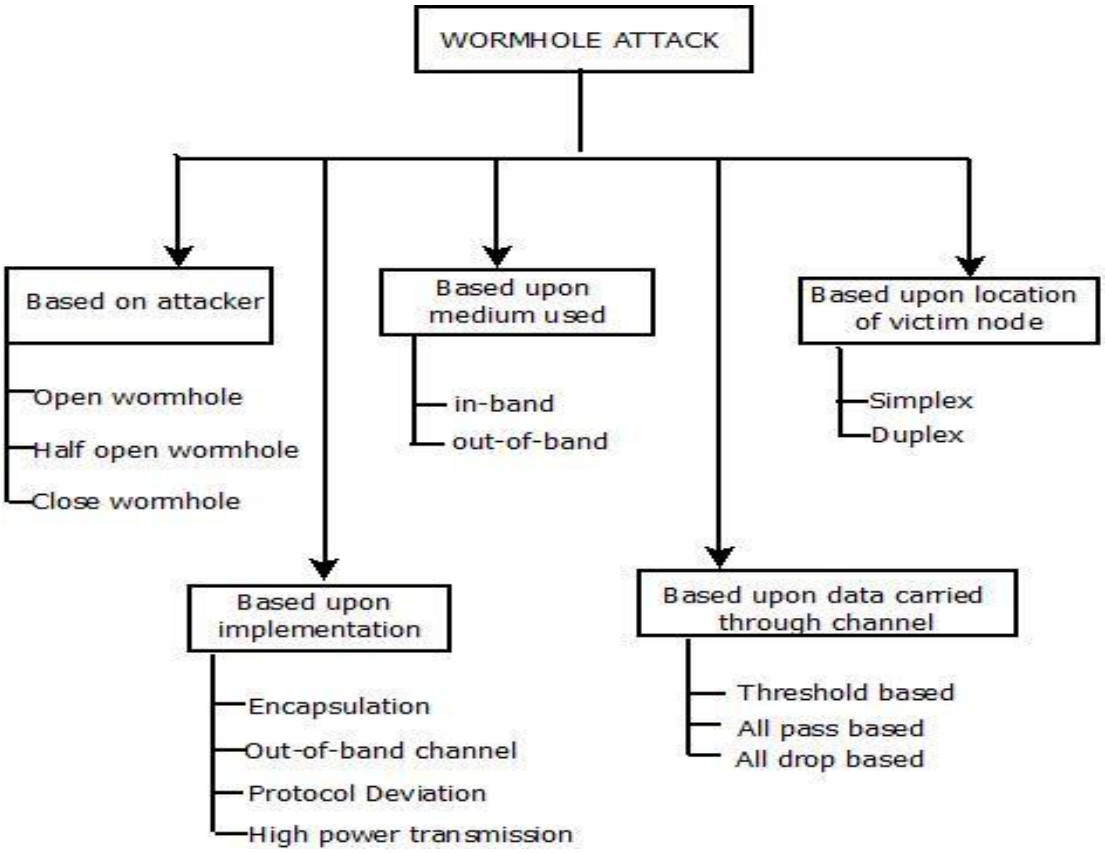

Figure 2: Taxonomy of wormhole attack

Section 2 presents description of service-oriented architecture and bilinear pairing. Related works describe in Section 3. Proposed scheme is described in Section 4. To show the effectiveness of the proposed approach, the experimental results and comparisons with various existing schemes are discussed in Section 5. Paper is concluded in Section 6.

SERVICE ORIENTED ARCHITECTURE

The aim of service oriented architecture [6-7] is to provide robust, easy to access and ready to use interface that maintain transparency among connected, semi-connected and disconnected nodes and the system thus developed is loosely coupled, has many joint services that provide light weighted application composition and development.

Such middleware architecture is useful in case when applications need more advanced functions to break complicate design and its architecture into smaller components.

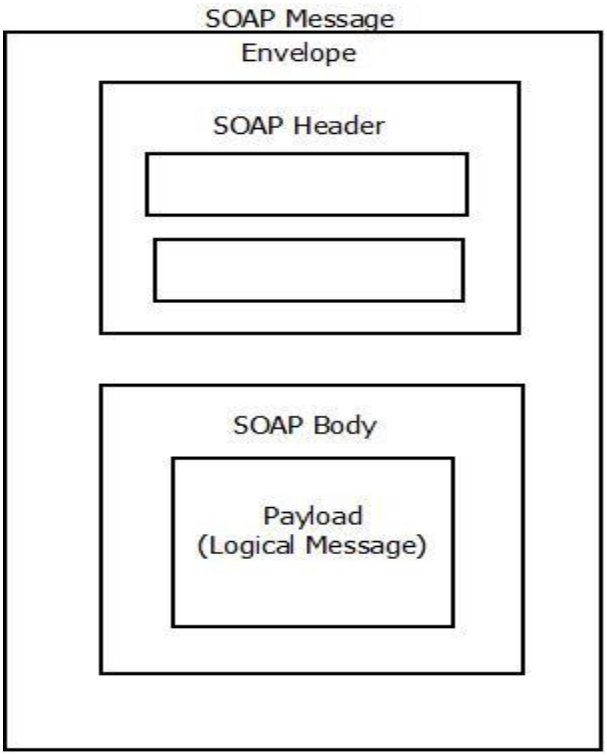

Figure 3: Service Oriented Architecture

The basic building blocks of any service oriented architecture are service provider, service broker and a service requester. They communicate through Simple Object Access Protocol viz. SOAP message whose format is described in Figure 3. Service provider develops new service modules as per the requirements of applications; service broker registers these services along with their descriptions in a structure called Universal Description Discovery and Integration viz. UDDI. Service requester requests for services from service broker, according to its requirements. The service contract is a specification through which consumer will interact with the provider. This middleware architecture can provide functional requirements like service creation, group management, communication, real-time application as well as non-functional requirements like interoperability, service discovery, and reusability of components.

Service description present in UDDI of service broker is written in WSDL (Web Service Description Language). WSDL is an XML based language and it describes services, location of services, operations performed by services (one-way, request-response, notification) and methods for accessing them so, UDDI is a directory of

web services interfaces that is described by WSDL. UDDI communicates through SOAP (Simple Object Access Protocol) described in Figure 4. SOAP is based on XML too. It is simple, extensible, platform independent and language independent. XML is used to carry and store data and as it is stored as plain text format, it can easily be shared among different applications and hence architecture developed is software and hardware independent [8].

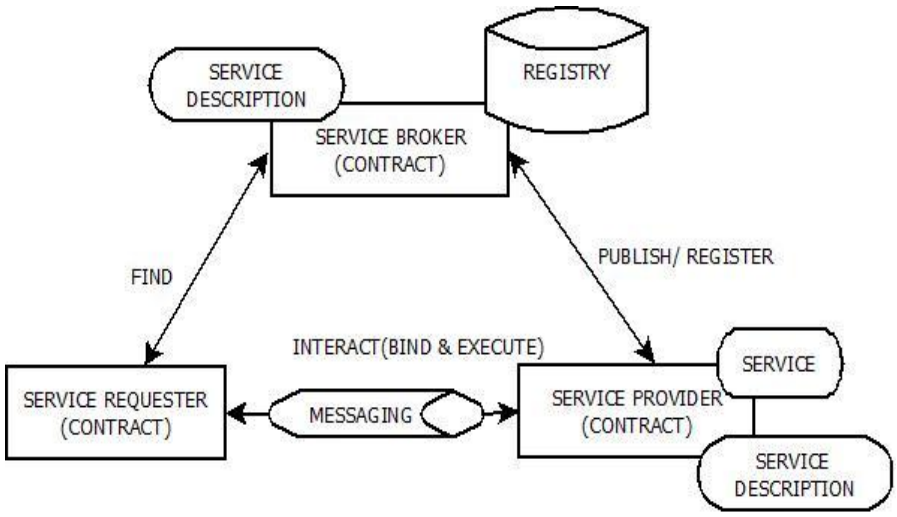

Figure 4: Communication in SOA

1.5 ISSUES OF MANET WITH SOA:

There are several advantages that could be obtained by using service oriented architecture [9-10]:

- **Heterogeneity:** It should provide a common interface to different hardware involved at different nodes.
- **Mobility:** As nodes belonging to MANET is not bound by any fix topology they establish routes dynamically so this architecture should provide a mechanism for adapting to changing traffic and propagation condition.
- **Scalability:** As the application gets bigger as per user demand; this architecture should provide a flexible base to add as many services as required.
- **Interoperability:** As the customer's demand are increasing so are the service broker and service provider to fulfill those demands and they use different platforms like C, JAVA etc. to build services so to form service composition for large application, interoperability is most characteristic.

- **Security:** some real time applications like those meant for military use carry very sensitive information so security module of this architecture should be capable enough to protect that information from malicious users.
- **Context awareness***:* Context means every such factor that has an impact on behavior of the application so the middleware to be used should be context aware. This awareness can be either related to the device or environment. If it device awareness, it is related to battery, processing power or memory management and if environment awareness, it's about connecting, bandwidth, location etc.

Properties of bilinear Paring:

- **Bilinear is pairing** [11]: Consider G_1 and G_2 are two groups of order m. Let $(G_1, +)$ be an additive cyclic group with generator *p* and $(G_2, *)$ be a multiplicative cyclic group with generator *q*.

Pairing: a: $G_1 * G_1 \rightarrow G_2$ with the following properties:

- **Bilinearity:** $\forall$ a,b $\in Zq^*$ and $\forall$ P,Q $\in G_1$: a (aP, bQ) = $a(P,Q)^{ab}$.
- **Non-Degeneracy:** There exists $\forall$ P, Q $\in$ G such that a (P, Q) $\neq$ 1, in other words for every pair of P,Q do not mapped to the identity in G_2.
- **Computability:** $\forall$ P, Q $\in$ G1, there is an efficient algorithm to compute e (P,Q). It is computable in polynomial time.
- **Computational Diffie-Hellman Problem (CDHP):** $\forall$ a,b $\in Zq^*$ to compute abP for given P, aP, bP.
- **Inverse Computational Diffie-Hellman Problem (Inv-CDHP):** $\forall$ a $\in$ Zq*, to compute $a^{-1}P$ for given P, aP [26-28].

RELATED WORKS

Qian *et al*. [12] gave a statistical analysis of multi-path (SAM) to detect wormhole attack & malicious nodes. The performance of multi-path routing in the presence of wormhole attack is analysed in cluster based and uniform network topologies. The results show that SAM detects wormhole attacks & identify the malicious nodes. Hu *et al*. [13*]* introduced a packet leashes based approach for detection & defending against wormhole attack. TESLA with Instant Key disclosure (TIK) provides instant authentication of received packets. TIK takes n public keys for network with n

number of nodes. It has relatively less storage, per packet size, and computational costs.

Lazos *et al*. [14] gave a graph theoretic approach for detecting and defending against wormholes. It also presents a defence mechanism using local broadcast keys and calculation the probabilities of detection. For detection of wormhole attack, it must use probabilistic techniques when absence of location or distance bounding.

Jain *et al.* [15] gave a novel trust-based scheme for detection & prevention of wormhole attack in the network without use of any cryptographic algorithm. The simulation results show that trust-based scheme is better in terms of packet dropping ratio and throughput.

Khalil *et al*. [16] introduced a lightweight countermeasure mechanism for detection & isolation of wormhole attack. This approach is suitable for resource constrained multi-hop wireless networks. Simulation results show that detection & isolation of wormhole attack every wormhole within a very short period of time in case of large range of scenarios. It also shows that this scheme have low resource consumption and detection latency.

Hu *et al*. [17] introduced prevention of wormhole attack using directional antennas. It diminishes threat of wormhole attacks and also requires no clock synchronization or location information. They are less expensive than other existing schemes for localization, and also provide in addition to security including more efficient use of spatial use of bandwidth and energy.

Zapata *et al.* [18] gave a secure AODV (SAODV) routing protocol for mobile ad hoc network. It uses a digital signature scheme for security purpose in mobile ad hoc network. Main drawback of SAODV is key distribution problem between the nodes.

Sanzgiri et al. [19] gave a ARAN protocol, which provides a secure routing in the infrastureless based network. It ensured some security goals such as authentication and non-repudiation using pre-determined cryptographic certificate. Simulation results show that ARAN is efficient protocol than AODV.

Sharma *et al*. [20] introduced prevention of wormhole attack by using identity based signature scheme on cluster based ad hoc network. This scheme does not require distribution cryptographic ertificate between the nodes so it decreases computation overhead. Simulation results show that prevented wormhole attack successfully and it also outperforms other existing schemes.

PROPOSED SOA BASED SCHEME

In this section, we proposed a SOA based signature scheme on cluster based MANET as shown in Figure 5. Ad hoc on-demand distance vector (AODV) routing protocol is used for communication between the nodes. A modified AODV routing protocol to cover all aspects of assumed scenario. Cluster head (CH) is assumed to be non-malicious. To implement service oriented architecture, CH is deployed as service broker and other nodes can either be service consumer or service provider depending upon the application requirement by a user. Figure 5 shows that how to SOA implemented over MANET. Any SOA mechanism can be appended with routing protocol or can be provided as separate layer above the network layer. Here, we have appended SOA modules with on-going mechanisms to provide security against wormhole attack. Cluster head works as private key generator (PKI). Time-to-live (TTL) is the average time required by any message to reach desired node in cluster of reasonable time. Service lease is the amount of time for which any consumer or provider can be bound in a cluster. Hence TTL will always be less than or equal to service lease. Table 1 shows that notations used in proposed model.

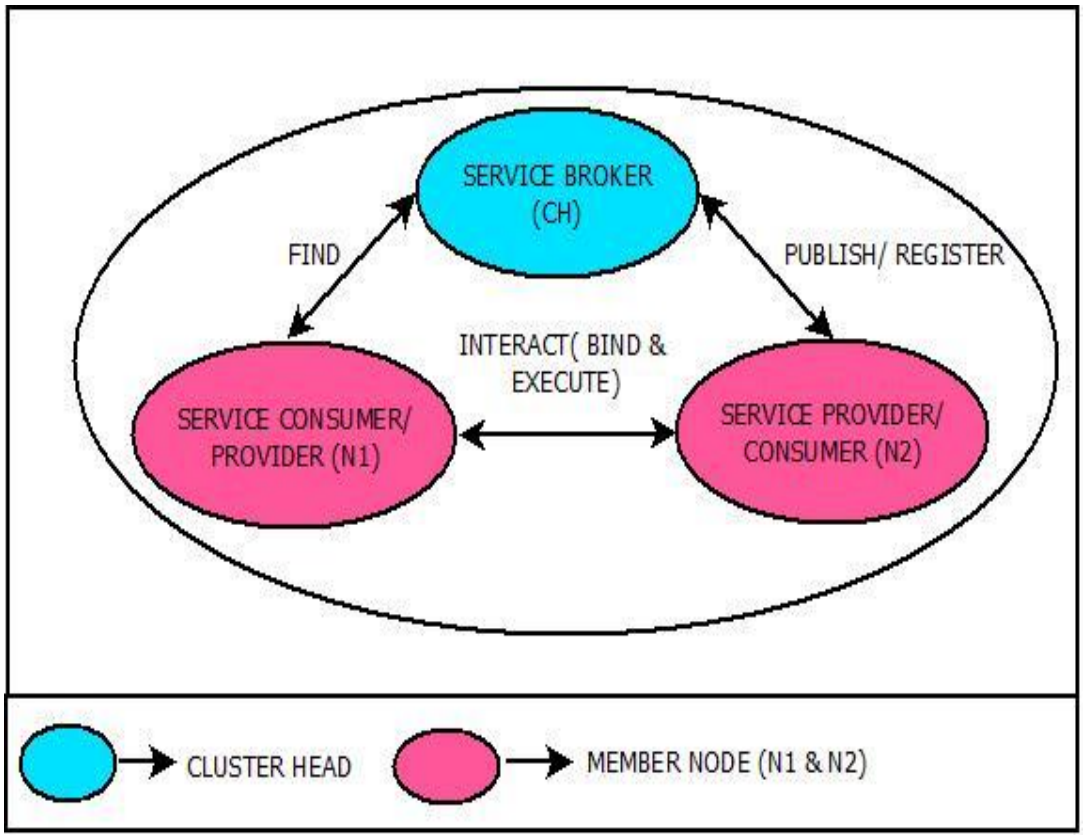

Figure 5: SOA in cluster based MANET

Proposed SOA based scheme consists of the following phases:

- Setup Phase
- Join Phase:
- Signature Generation Phase:
- Verification Phase
- Communication Phase
- Removal phase

Setup phase: Setup phase uses following steps:

i. A service broker broadcasts cluster parameters (SB_{skey}, G_1, G_2, m, a, H, p, q, CH_{pkey}) in the entire network through publish-subscribe channel as in Figure 6.

ii. Upon receiving cluster parameters, a service consumer sends their identity (ID) to respective service broker.

iii. A service broker performs following operations:

Public key generation: $Pub_i = H(ID_i)$, where $1 \le i \le N$.

Private key generation: $\Pr v_i = Pub_i \times \left(SB_{skey} / s \right)$

iv. A service broker sends private keys to corresponding service consumer via secure channel.

Table 1: Notations

Notation	Meaning
SB_{skey}	Service broker secret key
SB_{pkey}	Service broker public key
p	Generator of group G_1
q	Generator of group G_2
H	Hash function, H:{0,1}*→Zq*
a	Bilinear mapping, a: G_1* G_2→G_2
G_1	Additive cyclic group of prime order m
G_2	Multiplicative cyclic group of prime order m
g	generator

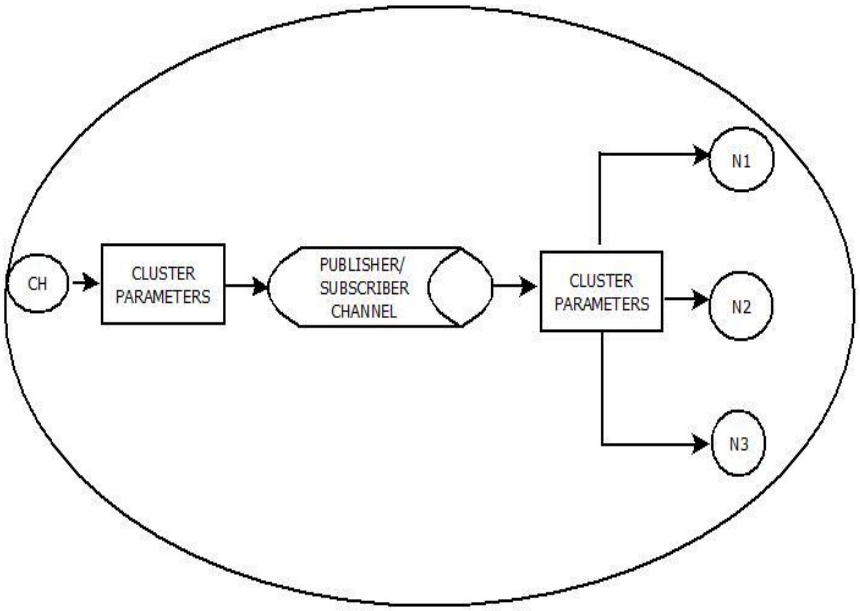

Figure 6: A service consumer distributes cluster parameters to all members

Join Phase:

- If any service consumer enters a particular cluster, it sends a join message to cluster head. After that it broadcasts own ID to all participating service consumers.
- Join message contains service description of services offered by that node.
- A service broker appends descriptions in UDDI registry. After that it performs all steps in setup phase.

Signature Generation Phase: A service consumer uses lists of steps in signature generation are as follows:

i. A mobile node works as service consumer in working scenario of proposed scheme. A service consumer selects random number $r_i \in Z_{q*}$ & computes the value of $V_{S_i} = g^{r_i}$, where $1 \le i \le n$.

ii. A service consumer broadcast Vs_i as a public parameter and value of r_i kept as secret.

iii. A service broker computes the following values:

$h_i = H_0(m_i)$

$S_i = (r_i + h_i)$.

iv. The combination of $\pi = (S_i + V_{S_i})$ is known as resultant signature on message *m*.

Verification Phase: A service broker uses list steps in signature generation phase are as follows:

i. A service broker works as a verifier in working scenario of proposed scheme. Upon receiving signature $\pi = (S_i, V_{S_i}, m_i, h_i)$ on message m_i where, $1 \le i \le n$. It checks correctness of signature on a signed RREP.

ii. A service broker checks the following condition:

$e(Pub, S_i) = (V_{S_i}, g^{h_i})$,where $1 \le i \le n$

iii. If the above condition holds then it is known as a fake signature.

Communication phase: A service broker wants to access security services. It requests to respective service provider for access required services through a command. Figure 7 shows that a service-oriented enterprise for notification about any event. All communicated message should follow request-reply format of simple object access protocol (SOAP).

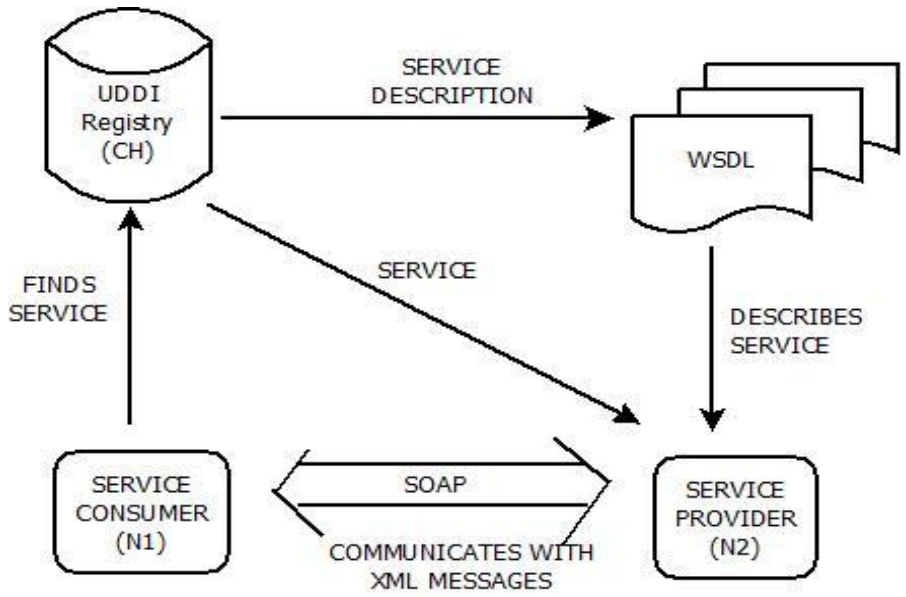

Figure 7: Communication between nodes

Intra-cluster communication:

i. A service consumer that wants to access services. It requests to service broker which would reply with service description to destination as in Figure 8.

ii.

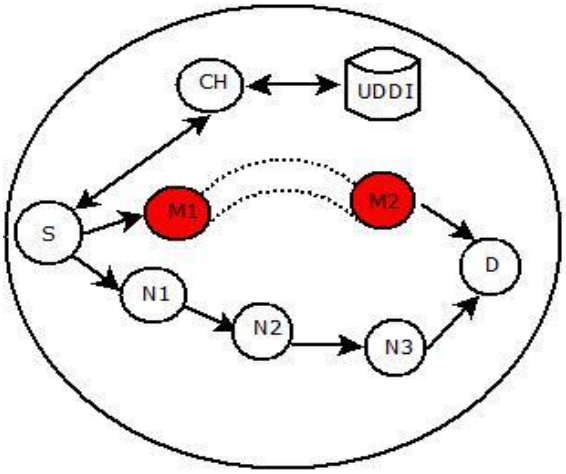

Figure 8: Intra cluster communication

iii. UDDI contains description of all web services.

iv. Consumer will now find the route to desired destination using AODV in modified form.

v. A RREQ will be sent to all neighboring nodes.

vi. If there is any malicious service consumers present with an intention to perform wormhole attack, it would immediately reply with low hop count and high destination sequence number.

vii. A Route confirm first (RCNF) packet will be created and It consists of four fields, namely, destination sequence number, hop count, identity(ID) and time to live value. This packet should be communicated in encrypted form.

viii. RCNF would be appended to another RREQ having request ID. It sets to two, which indicates two requests from same source and D flag set to one to indicate this packet is only meant for destination to interpret. These fields would also be encrypted.

ix. An intermediate service consumer would only increment hop count as they forward packet to their neighbors along with specified route in packet. If any such node would be wormhole, it would again try to fabrication of a packet, it able to do so on a RREQ packet but RCNF packet would remain unaffected.

x. When it would reach destination, it would match corresponding fields of both the packet, if any of the value shows a difference RERR packet would be generated with ID of malicious node obtained from RCNF. Malicious node will be blacklisted and all the routes through that node would no longer be used.

xi. If there is no violation of protocol RREP would be generated which would backtrack to the source.

Inter cluster communication*:* In inter cluster communications similar procedure would be used.

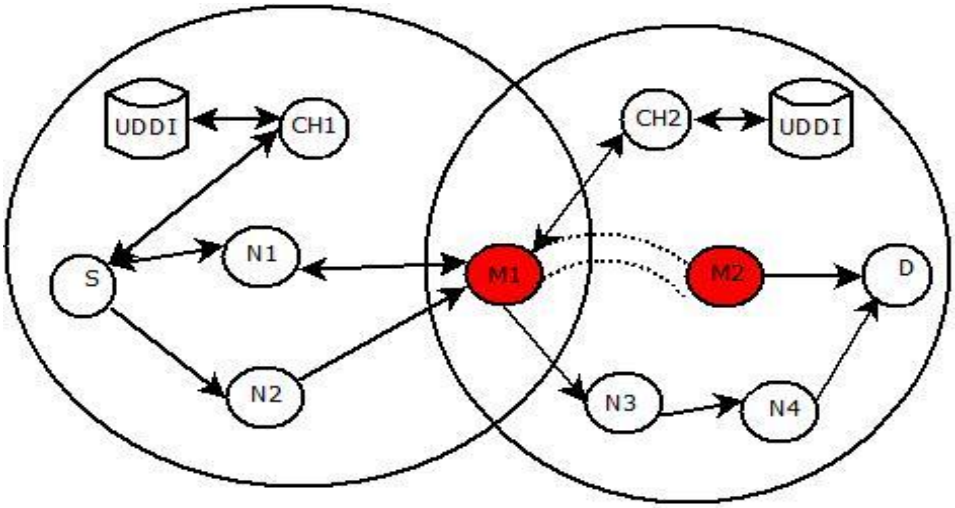

Figure 9: Inter cluster communication

As service broker has service description of every service available through nodes of that particular cluster so if on sending service request message, generated reply would be service not found than sender would go for inter cluster communication in Figure 9.

i. A service consumer having ($SB_{skey,}$ SB_{pkey}) pair same as original sender belong to same cluster hence they would act as router and keep on forwarding the request.

ii. When the service request reaches any of the boundary nodes it would be sent to service broker of adjacent cluster as boundary nodes will contain ($SB_{skey,}$ SB_{pkey}) pair of all those clusters of which it is member.

So any of service brokers having description of desired service will reply back and remaining procedure would be same as intra cluster communication.

Removal phase:

i. When a service consumer wants to leave a cluster, it has to send signed remove message to service broker because it can prevent from attacker who tries to impersonate the sender and can send fake removal message to cause denial of service attack.

ii. Service broker checks its registry and removes all the entry corresponding to that particular node.

Table 2. Notations used in Algorithm 1

Term	**Details**
RREQ	Route request
N	No. of nodes
S	Service consumer
RERR	Route error
IN	Intermediate node
D	Service provider
RCNF	Route confirm packet
TTL	Time to live
destseqnum	Destination sequence number
RREP	Route reply

In this approach, a service broker can be bottleneck so to avoid data loss. Each cluster member has mirror image of UDDI registry. If service broker gets down, a service consumer having mirror image of UDDI registry and some other node will be holding replica. When size of UDDI registry exceeds the threshold value, then we applied indexing with index copy present in service broker while fragments can be scattered on different node to allow distributed storage. Table 2 shows notations used in Algorithm 1.

Algorithm 1: **Prevention of Wormhole attack**

$S \xrightarrow{RREQ} D$

for i=1 to N do

if(**IN!=S) /* it** has valid route to **D */**

if (**destseqnum** of **IN** >= **destseqnum** of RREQ)

$D \xrightarrow{RREP} S$

else

Forward a **RREQ** to its neighbour

if (RREP is received by **S**)

Create **RCNF** packet (**destseqnum, hopcount**, **TTL, ID)**

Encapsulate **RCNF** by $\mathbf{Prv_{sc}}$ & finally encrypted with Pub_{sc}

Create new **RREQ** which having D=1 and **reqID**=2

Send new (**RREQ + RCNF)** to D

if TTL expires then

S sends new **RREQ + RCNF$_1$** more time and if **TTL** expires again **RERR** message would be generated to discard the routes through nodes mentioned in **RREP**.

else

for i=1 to N, if **IN!= D**, every **IN** increments **hop count** by 1 and forward toward **D** do

When **D** receives **RCNF**+ new **RREQ**, it decrypted by $\mathbf{Prv_{sp}}$ and Pub_{sc}

if field values of **RCNF**== field values of new **RREQ**

Send **RREP** to service consumer

else

Send route error (**RERR)** to a service consumer **S** for discarding nodes in suggested path

end if

end if

end if

end if

end if

PERFORMANCE EVALUATION

In this section, we use SOA based signature to mitigate wormhole attack, which is simulated under ns-2. We have used AODV with certain modifications as routing protocol. Table 3 shows the parameters during simulation.

Table 3: Simulation Parameters

Parameter	Value
Simulation Software	ns-2
Simulation area	500 X 500
No. of nodes	10 to 100
Simulation Time	500 s
Routing protocol	AODV
Maximum speed Traffic agent	15 m/s
Pause time	6 s
Node speed	2-10 m/s
Size of data packet	512 bytes
Transmission coverage	250 m
Mobility Model	Random waypoint Model
No. of Malicious nodes	2

Performance Metrics:

Performance metrics that have been used to evaluate performance of proposed scheme are:

Packet Delivery Ratio (PDR): It is ratio of total number of packets being sent by a source and total number of packet received at destination end.

End-to-end delay: It is average time taken by a data packet that was successfully delivered at the destination end.

Throughput: It is ratio of total number of data packets successfully transferred at destination end and simulation time.

Simulation Results:

Figure 10 shows that a comparison graph between *SAODV*, ID based scheme, and SOA based scheme using packet delivery ratio (*PDR*) as a performance metric. The simulation result shows that proposed scheme is having *97.28%* while S*AODV* and ID based scheme having *94.40 %* and *95.11 %* for average packet delivery ratio (*PDR*). The simulation result shows that proposed SOA based scheme is better than other two schemes.

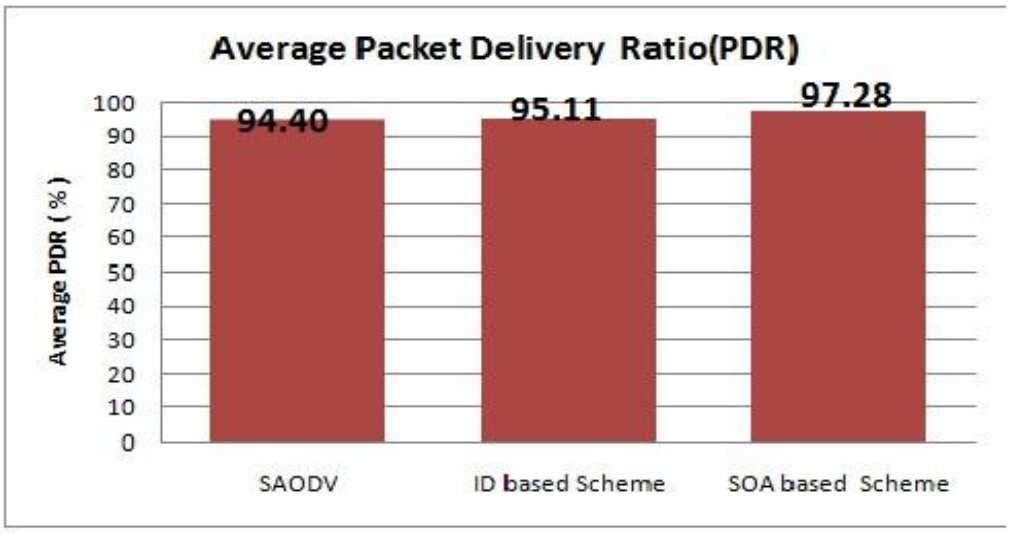

Figure 10: Packet Delivery Ratio

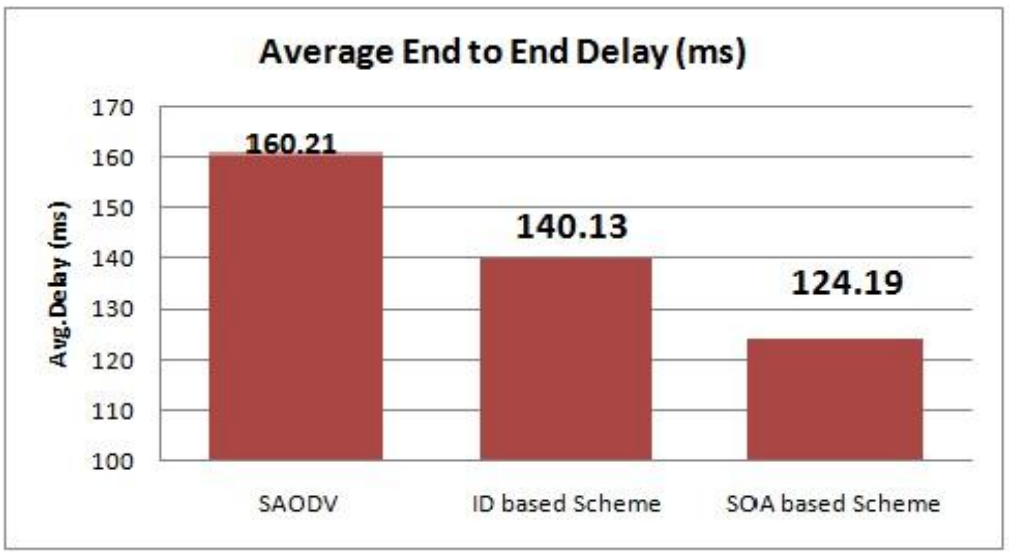

Figure 11: Average End to End Delay

Figure 11 shows the comparison graph for above three schemes on average end-to-end delay. SAODV takes 160.21 ms, ID based scheme takes 140.13 ms while the proposed SOA scheme takes only 124.19 ms on end-to-end delay. Hence proposed *SOA based* scheme perform better than other existing schemes such as S*AODV* and *ID based scheme*.

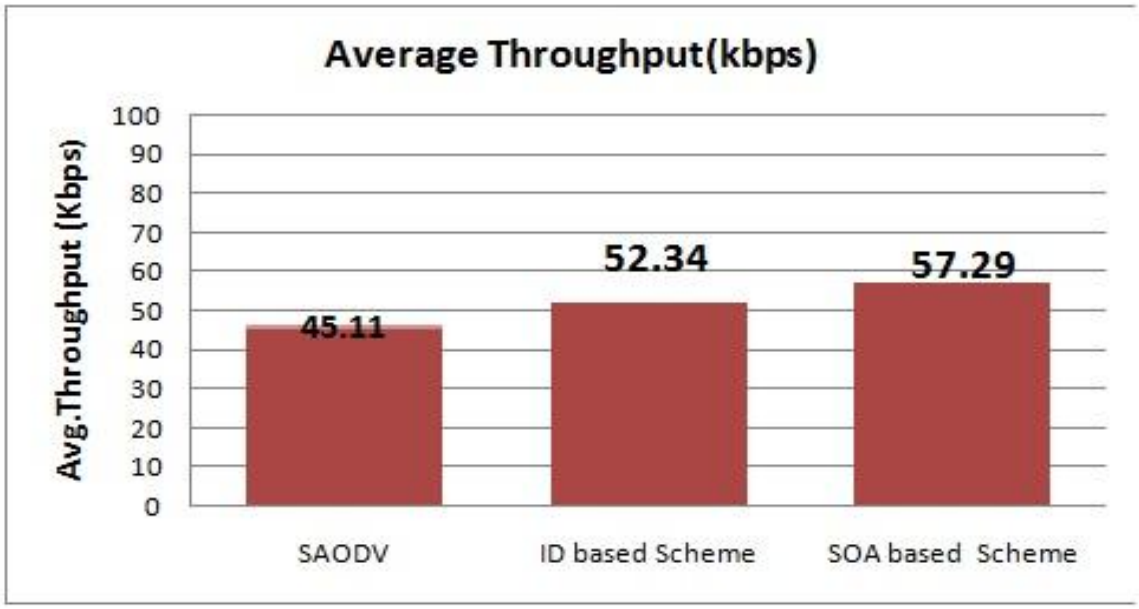

Figure 12. Average Throughput

The outcome of simulation is calculated for throughput for other existing schemes in Fig. 12. Standard SAODV has 45.11 Kbps, ID based scheme has 52.34 Kbps while proposed SOA based scheme has 57.29 Kbps for throughput parameter.

Comparison of security: In this section, we have compared our proposed approach with various existing approaches to point out the benefits achieved by using the SOA based signature scheme as in Table 2.

Table 2: A comparison between existing and proposed scheme

Existing Schemes / Parameters	ARIDANE[13]	ARAN[19]	SAODV[18]	ID based Scheme[20]	Our scheme
Authentication	✓	✓	✓	✓	✓
Integrity	✓	✓	✓	✓	✓
Non-repudiation	X	✓	✓	✓	✓
Mobility	X	✓	✓	✓	✓
Secrecy	X	X	X	✓	✓
Level of error detection	…	…	…	…	✓
Heterogeneity	…	…	…	…	✓
Coupling	…	…	…	…	✓
Flexibility	…	…	…	…	✓
Scalability	…	…	…	…	✓
Reusability	…	…	…	…	✓
Platform-independence	X	X	X	…	✓
Certificateless	X	**X**	X	…	✓
Low computation cost	X	X	X	✓	✓

The parameters used for comparison include security goals such as authentication, non-repudiation, integrity and secrecy. Proposed approach consists of identity based signature and SOA based approach. Identity based approach is used for achieving security goals. SOA base approach is used for flexibility, scalability.

CONCLUSION AND FUTURE SCOPE

Proposed approach has three modules viz., service provider, service broker and service consumer that can easily be deployed on any platform irrespective of hardware & software. This approach uses an identity based signature and SOA scheme. Identity based signature scheme is used for ensuring security goals & prevention of wormhole attack while SOA based scheme is used for achieving

interoperability, flexibility, heterogeneity, coupling, platform-independence, scalability and reusability on a cluster based MANET. Hence, proposed scheme is an effective way of providing security against wormhole attack in a network. However, when overall network conditions are taken into consideration then computation cost gets increased due to high mobility of nodes. Therefore, signature computation phase extends longer and hence overall communication time gets increased. Hence, further work will focus to minimize computation time. Although the approach successfully prevents a network of wormhole attack launched through protocol distortion, but still there are other approaches such as in-band, encapsulation. They cannot mitigate wormhole attack. Therefore, this issue shall also be addressed in future work.

REFERENCES

[1] Ci, S., and H. H. Chen, 2006. Self-Regulating Network Utilization in Mobile AdHoc Wireless Networks,. IEEE Trans. Vehic. Tech., 55: 1302–10.

[2] Hu, Y.-C., A. Perrig, and D. B. Johnson, 2006. Wormhole Attacks in Wireless Networks, Selected Areas of Communications. IEEE J., 24: 370-380.

[3] Mahajan, V., M. Natu.and A., Sethi, 2008. Analysis of wormhole intrusion attacks in MANETS. IEEE Military. Comm. Conf. (MILCOM), 1-7.

[4] Chiu, H.S., and K. Lui, 2006. DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks. Int. Symposium on Wireless Pervasive Computing, 1-6.

[5] Maulik, R., and N. Chaki, 2010. A Comprehensive Review on Wormhole Attacks in MANET. Int. Conf. on Com. Info. Syst. and Industrial Management Applications, 233-238.

[6] Booth, D., H., Haas, F., McCabe, E., Newcomer, M., Champion, C., Ferris, & D., Orchard, 2006. Web Services Architecture. W3C Working Group Note 11.

[7] MacKenzie, C., K., Laskey, F., McCabe, P., Brown and R., Metz, 2006. Reference model for service oriented architecture. OASIS Committee Draft 1.0.

[8] Chowdhury, M., K. H., Samsuzzaman, M., Islam, T., and Solaiman, B. M., 2012. Proposed technique of XML base secured data encryption and transmission technology. World Applied Sci. J., 20*:941-945*.

[9] Mascolo, C., Capra, L., Zachariadis,S., Emmerich,W., 2002. XMIDDLE: A Data-Sharing Middleware for Mobile Computing. Wireless Personal Com., 77-103.

[10] Janakiram,D., and Venkateswarlu, R., 2005. A Distributed Compositional Language for Wireless Sensor Networks. IEEE Conf. on Enabling Tech. for Smart Appliances (ETSA), 1-11.

[11] Kumar, V., and R., Kumar, 2015. An Optimal Authentication Protocol Using Certificateless ID-Based Signature in MANET. Security in Comp. & Comm., 536: 110–112, 2015.

[12] Qian, L., and N., Song, X. Li, 2005. Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path. IEEE Wireless Comm., & Net. Conf., 2106-2111.

[13] Hu, Y.C., and A. Perrig, 2005. Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks. Springer, Wireless Net. 11: 21–38.

[14] Lazos, L., Poovendran, R., Meadows, C., Syverson, P., Chang, L., W., 2005. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. IEEE, Wireless Comm. & Net. Conf., 1193-1199.

[15] Jain, S., and S., Jain, 2010. Detection and prevention of wormhole attack in mobile adhoc networks. Int., J., of Comp., Theory and Eng., 2:1793-8201.

[16] Khalil, I., S., Bagchi, and N.B. Shroff, 2005. LITEWORP: Detection and Isolation of theWormhole Attack in Static Multihop Wireless Networks. IEEE, Int., Conf., on Dependable Sys. & Net. 1-10.

[17] Hu, L., and D. Evans, 2004. Using Directional Antennas to Prevent Wormhole Attacks. Proc. Network and Distributed System Symposium (NDSS), 1-11.

[18] Zapata, M. G., and N. Asokan, 2002. Securing Ad hoc Routing Protocols. Proc. ACM Workshop on Wireless Security (WiSe), ACM, 1-10.

[19] Sanzgiri, K., and B. Dahill, 2002.A Secure Routing Protocol for Ad Hoc Networks. IEEE, Int. Conf. on Net. Protocols, 1-10.

[20] Sharma, D., V. Kumar, and R. Kumar, 2016. Prevention of Wormhole Attack Using Identity Based Signature Scheme in MANET. Comput. Int. in Data Mining, 475-485.