Re-Authentication in Wireless Sensor Network

T. Pon Selvalingam
Assistant Professor
Department of Computer Science and Engineering
PET Engineering College
Vallioor

Siva Mahalakshmi
Assistant Professor
Department of Computer Science and Engineering
PET Engineering College
Vallioor

S. Kurshid Jinna, PhD.
Professor and Head
Department of Computer Science and Engineering
PET Engineering College
Vallioor

ABSTRACT

In an unprotected environment of Wireless Sensor Network, the authentication scheme for multicast secure communication has to be designed with limited usage of resources and computation. In Multicast Authentication Based on Batch Signature-Enhanced (MABS-E) scheme, a tree construction to counteract the Denial of Service (DoS) attack requires latency at the sender. This authentication latency leads to the jitter effect on real-time applications at the receiver. In few applications, user mobility is considered for authentication process. And also, due to user mobility, the sensor node is compromised. This paper proposes a technique called Batch based Selective Bin Verification (BSBV), which avoids the construction of merkle tree. It reduces latency and allows the receiver to tolerate DoS attack even in the case where the attack fails to be detected. In order to prevent to compromise a node, re-authentication scheme is employed, can prolong the lifetime of the sensor network is provided. The number of inspections of each packet is decreased when binning technique is used. In BSBV technique, the packet failure rate is decreased to 0.01 from 0.04 because all are verified with the batch verification, when the chosen bin is two. The Packet Delivery Ratio is 82.95% when fifteen malicious nodes are presented.

Index Terms—Multicast, Authentication, Signature, Re-authentication, Membership verification

1. INTRODUCTION

With advanced technological and biological weapons of today's society, authentication, in distance oriented communications and business transactions, is an important property of network security. If not, an adversary with sharp sword will intercept the communication and try to attack the information. Probability of attack in a wired medium is comparatively small. But in wireless medium, communicants should always alert and try to prevent or protect the transferring data from third party. In Wireless Sensor Network (WSN), an emerging multi focused research field, uses spatially distributed tiny sensing devices independently called node. In order to provide an effective integrity, confidentiality, authentication during communication, the need of security issues emerges in WSN. The sensor nodes are having distinct characteristics like low processing power and radio ranges, permit low energy consumption, and perform limited and specific monitoring and sensing functions. The following five features should be considered while developing sensor networks are scalability, security, reliability, self-healing and robustness.

Because of different characteristics and deployment in commonplace, communication and security of these networks are emerges as a critical concern. So, it is necessary to use effective mechanisms to protect sensor nodes from attack and secure communication schemes are required to communicate among each other or with base station. Much of the current research in sensor networks has focused on protocols and authentication schemes for protecting the transmitting information. Digital signature, is a mathematical scheme, may be used to authenticate a source of digital document and it provides non-repudiation. It is commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.The efficient method to deliver data from a sender to a group of receivers is multicasting. Multicast authentication may provide three security services such as data integrity, data origin authentication and non-repudiation. The sender generates a signature for each packet with its private key, which is called signing, and each receiver checks the validity of the signature with the sender's public key, which is called verifying. If the verification succeeds, the receiver knows the packet is authentic. The authentication of multicast transmissions of data streams over the internet is a challenging problem. This is implemented with a best-effort delivery mechanism over the UDP transport protocol [13]. Thus, the received stream may differ from the transmitted one. Any authentication scheme for multicast streams should verify as many as possible of the received packets without assuming the availability of the entire original stream. The following issues in real world challenging the design. First, each receiver has to collect an entire block with a block signature before authenticating every packet in the block. A larger block size, chosen by sender, achieves higher computational efficiency and incurs longer latency for authentication [6]. Second, the relationship between the packets of each block due to the hashes or coding [13] makes the stream vulnerable to packet loss in the sense that the loss of some packets makes the other packets unable to be authenticated. In an extreme case, the loss of the block signature makes the whole block of packets unable to be authenticated. Third, the ideal approach of signing and verifying each packet independently raises a serious challenge to resource-constrained devices. In order to reduce computation overhead, conventional schemes use efficient signature algorithms and are vulnerable to packet injection by malicious attackers. These forged packets can consume the receiver's resource, leading to Denial of Service (DoS). It costs extra computation overhead at receivers.

In view of the problems regarding the sender-favoured block-based approach [13], Multicast Authentication based on Batch Signature (MABS) [6] conceives a receiver-oriented approach by taking into account the heterogeneity of the receivers. The basic scheme (MABS-B) described in [6], uses batch signature which supports to verify the signatures of any number of packets simultaneously. The batch signature scheme

effectively reduces the delay in authentication, eliminates the correlation among packets and thus provides the perfect resilience to packet loss. The computation complexity of batch verification comes with the fact that there are some additional costs on processing for multiple packets. The major concern is that as the batch size increases, the computation cost also increases which is higher than the cost involved in final signature verification. However, it is not the case in reality. The merit of batch signature is that the batch size is chosen by each receiver, which can optimize its own batch size, so that the batch size will not be unmanageably large. The main disadvantage of MABS-E [6] is the latency at the sender. This authentication latency can lead to the jitter effect on real-time applications at the receiver. And also, due to user mobility, the sensor node can be compromised. Without constructing a merkle tree, it is possible to find and reduce the effects of a DoS attack even in the case where the attack fails to be detected is described using selective bin verification [26], [28]. The proposed mechanism is a combination of batch signature and selective bin verification called Batch based Selective Bin Verification (BSBV), in which the verification utilizes a set of *n* bins. In order to prevent node compromise, re-authentication is provided. The mobile node should again perform authentication procedure, after which the node moves to another location. This re-authentication protocol in [2] is lightweight in order to reduce the cost of re-authentication procedure. The merit of re-authentication protocol is that, it can reconstruct the sensor network in short time even if the network failure occurs. Re-authentication protocol provides other security-related features such as mutual authentication, non-linkability, data confidentiality, integrity and accountability.

2. RELATED WORKS

Authentication is provided in [5], [23] using symmetric key based schemes and these are resisting against impersonation and collusion attacks, but it is unable to avert the Identification Replication and energy depletion attacks. Using public key based schemes [8], [12], immediate authentication is achieved and reduces the costs of both computation and communication. Also, it overcomes the vulnerabilities presented in [5]. The main concern of these schemes is the energy spent on message propagation. Conventional block-based authentication schemes [13] can achieve computational efficiency at receiver's end. However, this scheme is unable to overcome the problem of packet loss and Denial of Service (DoS) attack. The schemes in [20], [26], [27] attempt to provide the DoS resilience alone. However, they still have the packet loss problem. But [6] provides a perfect resilience to packet loss and DoS attack by using batch signature with packet filtering mechanism. In packet filtering mechanism, the sender introduces the latency which leads to jitter effect. The comparison of these schemes is shown in Table 1.The hash-based authentication schemes presented in [17], [26], have the option to place the signature packet at the end or beginning of the stream. The technique in [17] introduces the additional packet overhead for the key hash because it eliminates the time synchronization requirement in [5]. A hash function is used to link the packets in a multicast stream with a signature. These schemes are not good enough to sign/verify the packets individually for delay-sensitive flows, such as packet video. By using BLS or DSA, MABS [6] can achieve more bandwidth efficiency than using RSA, and conventional schemes using a large number of hashes.

The communication overhead can be mitigated by amortizing a single signature across several packets. Another signature amortization scheme is based on an information dispersal algorithm that can tolerate a certain amount of packet loss. Recent efforts on signature amortization for multicast authentication have involved distillation codes [26]. A multicast authentication scheme based on a combination of digital signatures, hashes, and error-correction codes is presented in [20] but it requires high computation cost. Several solution approaches were proposed to address the problem of time synchronization [20] based approach such as TESLA and signature amortization scheme [26].Conventional authentication schemes [5], [8], [12], [17] are insufficient for solving the security conflicts in [20], [22]. The schemes presented in [1] are directly supporting hash function and the en-route filtering capability to solve the above security conflicts. But, these schemes are inefficient in terms of both computation and communication cost, when compared with [8], [12]. The technique introduced in [25] allows the receiver to tolerate large DoS attack while providing service to legitimate senders. Rather than process all the arriving packets, a host using the technique in [27], which processes only a subset of the received packets. However, due to the asymmetry in the cost of sending versus processing messages, the large reduction in processing cost outweighs the increase in network traffic during an attack. Timed Efficient Stream Loss-tolerant Authentication (TESLA) [5], [20] is susceptible to DoS attack and it is not suited for delay-sensitive applications. A scheme discussed in [22] utilizes two techniques based on distillation codes and it uses one-time password [19] to overcome the CPU overhead and is perfect resistance against DoS attack respectively. It increases the burden at the sender side and unable to provide non-repudiation. Distillation codes [26] are robust against pollution attack, a powerful class of DoS attack in which adversaries insert invalid symbols during the decoding process. A set of mechanisms available for providing authentication requires communication cost, computation cost and security. A tree-based authentication scheme and suffers from a high amount of overhead on the non-signature packets. The new protocols discussed in [4], [5], [9], [10], [11], [18], [23], [26] for authenticating the mobile users and it enjoys better computation efficiency and security like [8], [12]. And also these schemes do not require long term secret keys on the server and not suited for the large power devices. Few of these protocols [5], [23], [26] are vulnerable to DoS attack [6], [20], [22], [25] and are not providing the best authentication strategy for wireless networks. Mobile authentication algorithms illustrated in [18] is the applications of public-key cryptosystems [8], [12]. The public-key protocols have different levels of security and complexity. The protocol presented in [2] uses homomorphic encryption scheme [24], to prevent the node compromise [14] which supports unlimited additive operations and one multiplicative operation on encrypted data.

An algorithm in [3] is based on the polynomial pool-based scheme, the probabilistic generation key pre distribution scheme and the Q-composite scheme [16]. These schemes provide a higher probability for non compromised sensors to establish a secure communication with the mobile sink than the schemes in [16]. An enhanced key exchange protocol is proposed in [10], provides anonymous remote authentication. The scheme proposed in [9] differs from [21] in the way that provides authentication with the help of client account index, which helps to realize client anonymity with no encryption operations. An ID-based signature scheme is followed the Weil pairing algorithm and is secure if the Diffie-Hellman problem

is hard. Comparing with [15], [19], the scheme proposed in [7] has lower computational complexity and it is particularly suitable for implementing the computational resource-constrained environment.

Table 1: Comparison of different authentication schemes

Analysis / Schemes	Computation cost	Communication cost	Security
Symmetric [5]	Less	Less	Medium
Asymmetric (certificate, merkle tree) [12]	High	High	-
Asymmetric (bloom filter) [8]	Less	Less	High
En route filtering [1]	High	High	High
Batch Signature [6]	Less	Less	High

3. PROPOSED WORK

Much of the current research in sensor networks has focused on authentication schemes for securing the message transmission. Although messages may often include information about the entity, that information may not be accurate. The research concerning DoS has focused almost exclusively on preventing malicious packets from reaching their intended targets. While such research is worthwhile and is useful for thwarting particular classes of attack, these approaches alone are not sufficient to protect service providers. Particularly for protocols in which the receiver has a high processing cost, traditional approaches fail to protect against attacks in which the adversary can overwhelm the receiver by sending malicious messages that appear entirely valid. To counteract DoS attack, a tree is constructed in MABS-E scheme [6], which introduces latency at the sender. And also, due to user mobility [24], the sensor node can be compromised.

3.1 Basic System Model

The sensor network is composed of a sender and several group of receivers. Each group has its own head and several sensor nodes. The sender, which has higher computational power, battery and storage resource compared to the other entities, sends its packets to sensor nodes within the network. These packets reach the sensor node via cluster head. For example, here 'n' groups are designed and each group consists of five members. It is not necessary that all the members in a particular group should have the same storage capacity, battery, and computation power. These characteristics may vary from one sensor node to another. Figure 1, shows the basic system model of a sensor network.

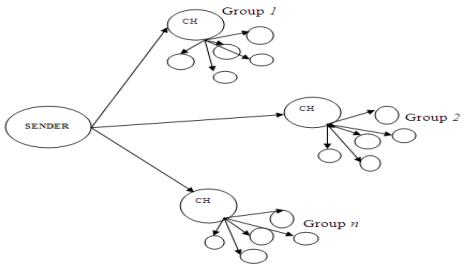

Fig 1. System Model

Multicasting information transformation with re-authentication using Batch based Selective Bin Verification (BSBV) is proposed. This mechanism uses AODV protocol for routing the data from one sender to a group of receivers and batch DSA algorithm [6] is used to create and verify the signatures simultaneously. Each sender transmits several packets (P_i), $\forall i = 1,2....l$ to a group of receivers. Each packet includes a message (M), signature *(Y)*, bin identifier *(b)*, sequence number *(c)*, sender address, receiver address and Time-To-Live (TTL). The sender signs each packet with a signature and transmits it to group of receivers through Ad-hoc On-Demand Distance Vector Routing (AODV) protocol. The AODV routing algorithm is capable of both unicast and multicast routing. It forms trees which connect to multicast group members. The proposed methodology starts with the signature creation at the sender side and the sender sends the packets with these signatures. Then the receiver queues the message in bins and performs the batch verification at the receiver side. If the output is high, then the authentication is provided. Otherwise, the packets get dropped. Also in WSN, user mobility is considered in authentication process. If the node moving from one place to another place, then the re-authentication is performed. This re-authentication is perfect resilience against node compromise. Figure 2 shows the flow diagram of overall proposed scheme.

3.2 Batch based Selective Bin Verification (BSBV)

Selective bin verification operates by processing only a randomly-selected subset of received messages. However, unlike sequential verification [26] in which all messages are stored in the same queue, bin verification utilizes a set of *n* bins, labeled $0.....n-1$. Upon receiving the packets, the receiver can apply the selective bin verification technique to cluster these packets and queues them in bin using $(b \bmod n)$. The bins are processed in ascending order of sizes. Attack packets are also processed and assigned to the bins in the same manner in which the original packets are processed. After some fixed amount of time (which we call the collection interval), the receiver chooses *k* bins called buffer bins, where $k \leq n$.

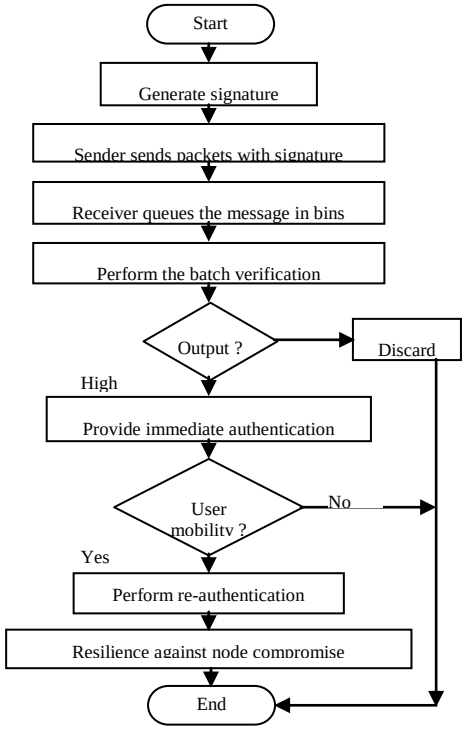

Fig 2. Flow Diagram of Proposed Scheme

Regardless of how bins are selected, the receiver proceeds by processing (verifying) each packet in buffer bins leads to high computation cost at receiver. Instead of each verification, this scheme utilizes the batch signature [13] which supports simultaneously verifying the signatures of any number of packets. Now the receiver proceeds by processing all packets in buffer bins with the batch verification [6], which achieves instantaneous authentication. Assume that the receiver collects l packets such as

$$P_i = \{M_i, Y_i\}, i = 1,2,....,l$$

It can input them into batch verification,

$$BatchVerify(P_1, P_2, ..., P_l) \in \{True, False\}$$

If the output is true, the receiver knows that the n packets are authentic, and otherwise not. The combination of both selective bin verification and batch signature technique is referred as Batch based Selective Bin Verification (BSBV).

3.2.1 System Architecture

The significant advantage of batch signature is that, the batch of packets is authenticated simultaneously through one batch signature verification operation. The packet independency also brings other benefits in terms of smaller latency and communication overhead.

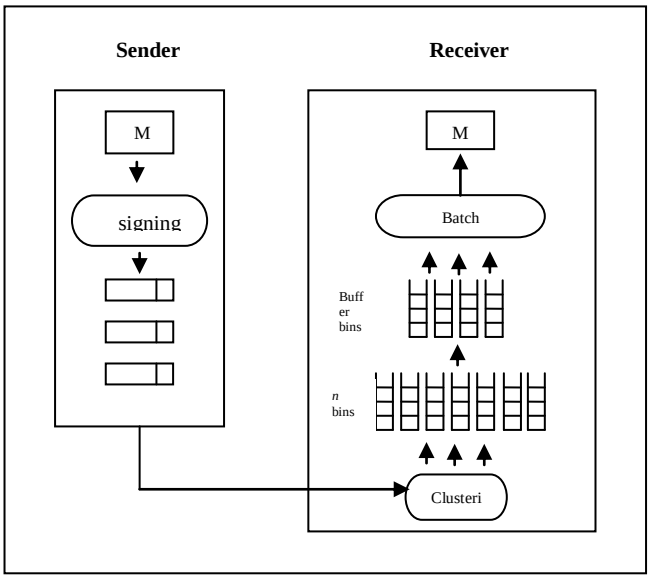

Fig 3. Overall processing of BSBV

Figure 3, shows the overall system architecture of proposed technique. The sender sends the packets and the receiver applies the selective bin verification technique to cluster these packets and queues them in bin. After the collection interval, the receiver chooses *k* bins where $k \leq n$. In order to reduce the computation cost, batch verification can be performed over each buffer bin. If the verification over one bin succeeds, the set of packets is authentic. Otherwise, the set of packets is forged and can be dropped without further verification on each packet.

3.2.2 Protection against DoS Attack

Consider a channel, with 20% average loss rate between the sender and receiver, supports an attack in which an adversary can send 500 fake signature packets per second. In bin verification, divide the spoofing efforts using distinct sequence numbers. For example, suppose the sender creates 10 signature packets numbered 1 through 10 in a given second.

The receiver waits long enough to receive some or all of these, together with up to 500 spoofed signature packets from an attacker. For at least 2 of the ten sequence numbers there will be no more than 102 spoofed and legitimate packets using that number. There is about a 93% probability that a legitimately signed packet is in this group of 102 packets. Thus the attacker is typically only able to force an additional 100 verifications with 500 spoofed packets.

In selective bin verification, the receiver proceeds by processing each packet in the buffer bins. Selective bin verification uses the metric called number of inspections, which is carried out by the receiver. Here, it defines an inspection to occur when the receiver processes the packets, regardless of whether the packets are legitimate, a duplicate, or invalid. Let *a* be the attack rate (i.e., the number of attack packets arriving at the receiver per second), *i* be the collection interval (measured in seconds), and *n* be the number of bins.

When binning is not used, then the expected number of inspections required for *m* senders is $insp = ai + m(1-l)$, where *l* is the loss probability of the sender.

For the binning technique, the *m* senders are expected to cause $m * p(1-l)(bb/n)$ inspections, where *p* denotes the number of packets sent by each sender and *bb* is the number of buffer bins inspected by the receiver. Since the receiver only inspects *bb* bins, the contribution of the DoS is $ai(bb/n)$. Thus, the expected number of inspections is $insp = (bb(m*c(1-l)+(a*i)))/n$

Thus, when the attack rate *a* is much larger than *n*, then the attack rate is diminished by a factor of bb/n.

$$((g^{\sum_{i=1}^{n} s_i r_i^{-1}} y^{\sum_{i=1}^{n} h_i r_i^{-1}}) \bmod p) \bmod q = \prod_{i=1}^{n} r_i \bmod q \quad (1)$$

The equation (1) is used to perform the batch verification. It includes a technique called signature preaggregation. Here, the additional processing of multiple packets is shifted from the time of final batch verification to the time of each packet reception. This makes the cost of final batch signature verification is exactly the same as that of original signature verification.

For batch-DSA, the aggregations of the message hashes and signatures $(\sum_{i=1}^{n} s_i r_i^{-1}, \sum_{i=1}^{n} h_i r_i^{-1}, \prod_{i=1}^{n} r_i)$ are inside the signature verification. Therefore, the cost of the aggregations is incurred with the final signature verification. If verification is performed using binning technique on every packet of each buffer bin, then it results a higher failure rate. Instead, if batch verification [6] is employed, the failure rate will be minimized.

Algorithm: Batch verification
Input: Set of packets, P_i
Output: Set of authenticated packets, $auth\_packets$
1. begin
2. b := Bin Identifier;
3. n := Total number of bins;
4. k := Number of chosen bins;
5. *in*:= Number of inspections;
6.cluster the packets based on sequence number;
7. repeat
8. $b := b\%n$;
9.repeat
10. if $b == i$ then
11. create n bins and put the corresponding packets in i^{th} bin;
12.end if;
13.repeat
14. $batchVerify(s_i, r_i)$; // Perform batch verification
15.*in*:= $inspection(r, i, s, n, k)$; // Calculate no.of inspections
16. until k;
17. until n;
18.until P_i;
19.return $auth\_packets$; // returning authenticated packets
20. end;

Procedure: Number of inspections
Input: Signature s_i, r_i, Number of bins *n*, Selected bins *k*
Output: Number of inspections $ninsp$
1. begin
2 $lossprob := 0.20;$
3. $ninsp := number\ of\ inspections;$
4. $in := s*(1-lossprob);$
5. $insp := in+(r*i);$
6. $ninsp := (insp*k)/n;$
7. return $ninsp$; // returning number of inspections
8. end;

Procedure: Verification
Input: Signature (s_i, r_i)
Output: Set of authenticated packets, $auth\_packets$
1. begin
2. s_i, r_i := Signature of i^{th} packet;
3. h_i := hash of i^{th} packet;
4. g := Generator of Z_p^*;
5. y := Public key ;
6. repeat
7. $mu1 := mu1 + pow(r_i, -1)$;
8. $mu2 := mu2 + h_i * pow(r_i, -1)$;
9. $ru1 := ru1 * r_i$; // aggregation of r_i value
10. until P_i;
11. $a := pow(g, mu1)$; // aggregation of $s_i r_i$ value
12. $b := pow(g, mu2)$; // aggregation of $h_i r_i$ value
13. $c := (ab \bmod p) \bmod q$;
14. $z := (ru1) \bmod q$;
15. if $z == c$ then
16. packets get authenticated;
17. else
18. drop the packets;
19 end if;
20. end;

3.3 Re-Authentication

Re-authentication protocol consists of three phases: token authorization, registration, and authentication. The notations used in this paper are illustrated in Table 1.

A. Token authorization phase

When an end-user becomes a subscriber of the target service provider, the end-user obtains proper authenticated token w_i from the service provider. To issue the token w_i, the service provider selects two random integers R_i and $r(0 \le r \le 2^{160}-1).$ and by using these two, the service provider computes the token [6], $w_i = \mathrm{E}[-r, PK_{BGN}, G] = g^{-r} \cdot h^{R_i}$ for each subscriber.

B. Registration phase

After token authorization phase, the end-user should register him/her with the base station in order to obtain nonce R_s. The base station verifies whether the end-user is a legitimate subscriber of the target service provider through membership verification [24]. If it is true, the sender sends R_s to the end-user.

C. Authentication Phase

Here, cluster head computes $K_{U,CH} = \mathrm{H}(R_s + 1 \| R_U)$. Using this key, the communication between the end-user and cluster head can be secure. Since R_s is only known to the cluster head and end-user, they can share a secret key $K_{U,CH}$ .Each cluster head in this re-authentication protocol should compute only two exponent operations, four hash operations, and two symmetric operations.

D. Resilience against node compromise

The major advantage of node capture is the acquisition of valid keys since the adversary can launch various attacks using these keys.

In the proposed work, the adversary can obtain $\mathrm{E}[-(\alpha-1)r, PK_{BGN}, G]$, $g^{-\alpha \cdot r \cdot SK_{BGN}}$, SK_{BGN}, $K_{U,CH}$, and R_s by compromising the nearby cluster head. Although the adversary can impersonate the nearby cluster head using this information, he/she cannot distinguish two different end-users.

Table 2: Notations

Also, the adversary cannot generate different $\mathrm{E}[-r, PK_{BGN}, G]$ unless participating the authentication process. From this point, this re-authentication protocol has resilience against node compromise.

Algorithm: Re-authentication
Input: node with mobility
Output: re-authenticated node, $reauth\_node$

1. begin
2. EU := End User;
3. SP := Service Provider;
4. w_i := tokens;
5. R_s := Random nonce;
6. if $EU \in SP$ then
7. begin
8. for each subscriber
9. calculate w_i;
10. end for;
11. end;
12. end if;
13. $memberVerify(w_i);$
14. if EU is legitimate subscriber then
15. sends R_s to EU ;
16. end if;
17. return $reauth\_node$;
18.end;

Procedure: Member verification
Input: Token w_i
Output: Member or not

1. begin
2. m := number of new subscribers;
3. repeat
4. calculate $c = f(w_i);$
5. if $c^{SK_{BGN}} == g^{-\alpha \cdot r \cdot SK_{BGN}}$ then
6. return TRUE;
7. else
8. return FALSE;
9. end if;
10. until m ;
11. end;

Notation	**Description**
S/U	Sender/End-user
PK_{BGN}	A public key under BGN encryption [6] owned by S
SK_{BGN}	A private key under BGN encryption [6] owned by S and distributed to all sensor nodes for membership verification
$K_{A,B}$	A shared secret key between entities *A* and *B*
$\mathrm{E}[m, PK_{BGN}, G]$	A message *m* is encrypted by the public key PK_{BGN} on cyclic group *G* and the cipher text is $g^m \cdot h^r$
$R^i or R_A^i, 1 \le i \le n$	A series of 64-bit nonces generated by entity *A*

4. SIMULATION RESULTS

The scenario size is chosen as $1000 \times 1000m$. The 50 nodes are spread randomly over the network to create several

groups. From these nodes, at most fifteen nodes are acting like malicious nodes. Traffic sources are calculated by Constant Bit Rate (CBR). The routing protocol used for the process is AODV.
The experimental setup and the fixed simulation parameters for proposed work are listed in Table 3.

To analyze the proposed scheme the following set of metrics such as Number of Inspections, Bins checked, Attack rate, Failure rate, Number of malicious node(s), Number of senders, Throughput and the Packet Delivery Ratio (PDR) are considered. In this section, the simulation results demonstrate the efficiency of the BSBV technique.

Table 3 Experimental Setup

Parameters	**Value**
Simulator	NS-2
Simulation Time	150ms
Number of Nodes	50
Transmission Protocol	TCP
Application Traffic	CBR
Propagation Model	Random Propagation
No. of malicious nodes	15
Routing protocol	AODV
MAC	802.11
Channel	Wireless Channel
Queue type	DropTail Queue
Attack Type	DoS attack
Number of groups formed	6
Number of members per group	5

Table 4 Number of Inspections

Total Number of Bins(bins)	**Number of Inspections(packets)**	
	k=3	**k=4**
5	62	83
15	21	28
25	12	17
35	9	12
45	7	9
55	6	8
65	5	6
75	4	6
85	4	5
95	3	4
100	3	4

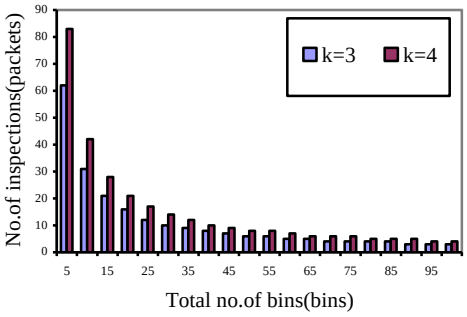

Fig 4 Number of Inspections

The analysis of the number of inspections is described in Table 4 and Figure 4 with respect to the total number of bins. To analyze the performance, proposed scheme uses the metric called number of inspections carried out by the receiver. Inspection is defined as it is occur when the receiver process the message, regardless of whether the message is legitimate, a duplicate, or invalid. Here, consider the maximum number of total bins as hundred. Two sets of number of inspections are analyzed for the chosen bins 3 and 4. For 5 and 100 numbers of bins, the maximum number of inspection is 62 and 3 respectively, when the chosen bin for the process is 3. When the total number of bins is increased, the number of inspections is decreased and becomes constant.

Table 5 Comparison of Binning and Non-binning technique

Attack Rate (attack/sec)	**Number of Inspections (packets)**	
	With Binning	**Without Binning**
10	22	74
20	37	124
30	52	174
40	67	224
50	82	274
60	97	324
70	112	374
80	127	424
90	142	474
100	157	524

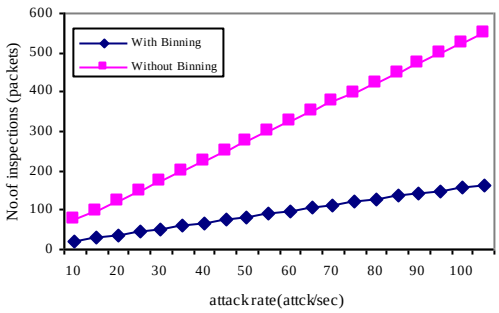

Fig 5. Comparison of Binning and Non-binning technique
Table 5 Failure rate with respect to bins checked

The analysis of number of inspections for the binning and non-binning approaches is described in Table 5 and Figure 5 with respect to attack rate. Attack rate is defined as the number of attack messages arriving at the receiver per second. The number of inspections is decreased when binning technique is used and increased when non-binning technique is used. Although both are linear, the slope resulting from the binning technique is significantly less than that of non-binning technique. From Figure 4.2 when the attack rate is 50, the number of inspections in binning technique is 82 and it is 274 in non-binning technique.

The analysis of throughput is shown in Table 6 and Figure 6 with respect to the number of malicious node(s). Throughput is defined as the average number of packets delivered successfully from source to destination per unit of time. Throughput is inversely proportional to the number of malicious node(s).

Table 6 Throughput

Number of packets sent	Number of packets received	Number of malicious node(s)	End Time	Through put (kbps)
2871	2581	1	28.97	587.71
5101	4708	3	52.78	569.84
8015	7563	5	60.59	536.16
10125	9605	7	79.88	520.44
10175	9666	9	80.63	505.48
11583	10886	11	90.49	497.19
14198	13349	13	110.51	451.80

Figure 6 shows, while the number of malicious node increases, throughput decreases. For example, when there are three malicious nodes, the number of packets sent is 5101 with the maximum throughput of 569.84 whereas for five malicious nodes the number of packets sent is increased with 7563 with the maximum throughput of 536.16. Thus, it is evident that, if the number of packets sent is increased as 2462 and the throughput decreased as 33.68, when the number of malicious nodes is increased from three to five.

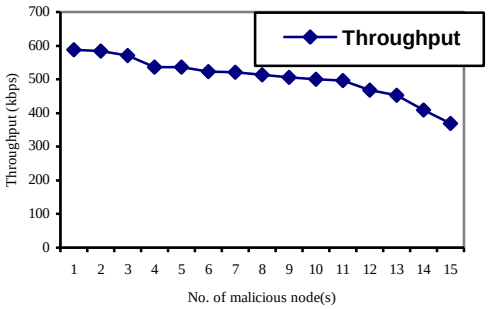

Fig 6 Throughput

Table 7 Failure rate with respect to bins checked

Bins checked	Failure rate	
	Per packet	Batch
2	0.04	0.010000000000000002
3	0.02	0.0010000000000000002
4	0.01	0.0010000000000000005
5	0.001	$1.0000000000000006e^{-5}$
6	0.0001	$1.0000000000000006e^{-6}$

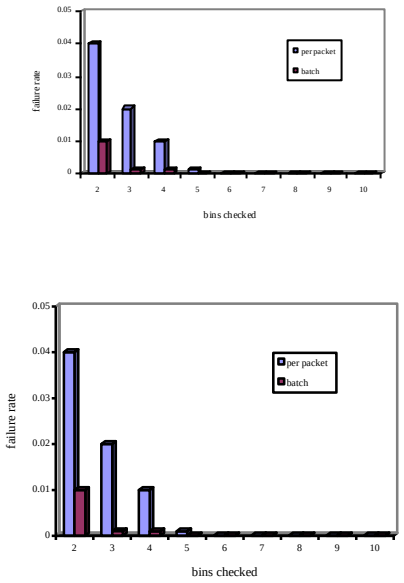

Fig 7 Failure rate with respect to bins checked

The analysis of failure rate is described in Table 7 and Figure 7 with respect to bins checked. Failure rate is referred as the probability of failure per unit of time; sometimes estimated as the ratio of the number of failures to the accumulated operating time for the items. Out of *n* bins only *k* bins are selected which is termed as bins checked. When compared with the existing model [26] failure rate is decreased in proposed model because the packets are verified with the batch verification. When the chosen bin is 2, the failure rate is 0.04 in [26] and in BSBV approach it is 0.01. The figure shows that the failure rate decreases as the bin check level increases. The variation is high only in primitive level, whereas the failure rate is maintained constant though the bin check is increased.

Table 8 Failure rate with respect to Number of senders

Number of senders	Failure rate
20	$1.0000000000000006e^{-6}$
40	$1.0000000000000014e^{-12}$
60	$1.0000000000000018e^{-18}$
80	$1.0000000000000025e^{-24}$
100	$1.0000000000000031e^{-30}$
120	$1.000000000000004e^{-36}$
140	$1.0000000000000045e^{-42}$

160	$1.0000000000000051e^{-48}$
180	$1.0000000000000058e^{-54}$
200	$1.000000000000006e^{-60}$

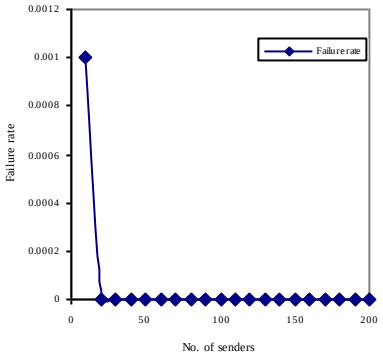

Fig 8 Failure rate with respect to Number of senders

The analysis of failure rate is described in Table 8 and Figure 8 with respect to number of senders. When the number of senders is increased, the failure rate is decreased. Here, the maximum number of senders is 200. In [26], the failure rate is 0.01 and in BSBV technique it is 0.001 when the number of senders is 10. So, the failure rate is minimum in the proposed scheme.

The analysis of Packet Delivery Ratio (PDR) is described in Table 9 and Figure 9 with respect to time. PDR is less, when a malicious node exists whereas it is high with the absence of malicious node. When the proposed scheme has been simulated with 15 malicious nodes which are attacking the traffic, PDR does not show much deviation of their performance but at primitive level. The ratios of the packets that are delivered to the receiver are dropped due to the presence of these attacker nodes. For 50 ms, the PDR is of 82.95% when the malicious node(s) are present whereas in the absence of malicious node(s) the ratio attains is 90.75%.

Table 9 Packet Delivery Ratio

Time(ms)	Packet Delivery Ratio (%)	
	Without Attack nodes	With Attack nodes
20	83.29	67.40
30	87.12	77.36
40	89.29	81.63
50	90.75	82.95
60	91.71	83.12
70	92.29	83.34
80	92.78	83.20
90	93.19	82.96
100	93.53	82.85

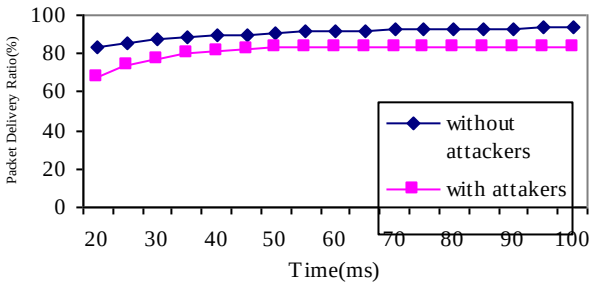

Fig 9 Packet Delivery Ratio

5. CONCLUSION

This proposed work has investigated the ability of Batch based Selective Bin Verification (BSBV) technique to protect services from attack without constructing a tree, even when the DoS flood reaches the receiver. Also, here, re-authentication protocol is used for membership verification and re-authentication of mobile nodes. Based on this method, an efficient and scalable re-authentication protocol over wireless sensor network is described. This protocol reduces communication overhead while increasing computational cost. The number of inspections is decreased when binning technique is used and increased when non-binning technique is used. When compared with the existing model [26], in the BSBV technique the packet failure rate is decreased because the packets are verified with the batch verification. The failure rate is 0.04 in [26] and in BSBV approach it is 0.01, when the chosen bin is two. For 50 ms, the Packet Delivery Ratio is of 82.95% when the fifteen malicious nodes are presented whereas in the absence of malicious nodes the ratio attains is 90.75%. The various other protocols such as dynamic source routing (DSR), Destination-Sequenced Distance Vector (DSDV) can be used to improve the performance of the network. BSBV follows a static method for fixing the selected bins. An extension to this work is to select the chosen bin dynamically. The re-authentication protocol can be applied for vehicular ad-hoc network.

6. REFERENCES

[1] Chia Mu Yu,"Constrained Function-Based Message Authentication for Sensor Networks," IEEE Transactions on Forensics and Information Security, Vol. 6, No. 2, pp. 407-425, Jun 2011.

[2] Jangseong Kim,"An Efficient and Scalable Re-authentication Protocol over Wireless Sensor Network," IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, pp. 516-522, May 2011.

[3] Amar Rasheed,"Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 1, pp. 176-184, Jan 2011.

[4] Chin Chen Chang,"An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks," IEEE Transactions on Wireless Communications, Vol. 9, No. 11, pp.3346-3353, Nov 2010.

[5] Taek young Kwon,"Secure and Efficient Broadcast Authentication in Wireless Sensor Networks," IEEE

Transactions on Computers, Vol. 59, No. 8, pp.1120-1133, Aug 2010.

[6] Yun Zhou,"MABS: Multicast Authentication based on Batch Signature," IEEE Transactions on Mobile Computing, Vol. 9, No. 7, pp. 982-993, Jul 2010.

[7] Dexin Yang and Bo Yang,"A Novel Two-Server Password Authentication Scheme with Provable Security," IEEE International Conference on Computer and Information Technology (CIT), Bradford, UK, Jul 1, pp. 1605-1609, 2010.

[8] Kui Ren,"Multi-User Broadcast Authentication in Wireless Sensor Networks," IEEE Transactions on Vehicular Technology, Vol. 58, No. 8, pp. 4554-4564, Oct 2009.

[9] Xuefei Cao,"Identity-Based Anonymous Remote Authentication for Value-Added Services in Mobile Networks," IEEE Transactions on Vehicular Technology, Vol. 58, No. 7, pp.3508-3517, Sep 2009.

[10] Yining Liu,"An Improved Anonymous Remote Authentication Protocol," Second International Symposium on Information Science and Engineering (ISISE), Shanghai, China, Dec 28, pp. 181-184, 2009.

[11] Guangming Dai, "An Effective Signature Scheme based on Tate Pairing for Mobile Business," International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08), Dalian, China, Oct 14, Vol. 8, No. 7, pp. 1-4, 2008.

[12] Kui Ren,"On Broadcast Authentication in Wireless Sensor Networks," IEEE Transactions on Wireless Communications, Vol. 6, No. 11, pp. 4136-4144, Nov 2007.

[13] Yun Zhou,"Multimedia Broadcast Authentication Based on Batch Signature," IEEE Communications Magazine, pp. 72-77, Vol. 45, No. 8, Aug 2007.

[14] Hui Song and Liang Xie,"Sensor Node Compromise Detection: The Location Perspective," In proceedings of International Conference on Wireless Communications and Mobile Computing (IWCMC'07), New York, USA, 12-16 Aug, pp. 242-247, 2007.

[15] Haimin Jin and S. Wang,"An Efficient Password-Only Two-Server Authenticated Key Exchange System," In proceedings of the 9th International Conference on Information and Communications Security (ICICS'07), Zhengzhou, Henan Province, China, Lecture Notes in Computer Science 4861, 12-15 Dec, pp. 44-56, 2007.

[16] S. Hussain, F. Kausar, and A. Massod,"An Efficient Key Distribution Scheme for Heterogeneous Sensor Networks," In Proceedings of International Conference on Wireless Communications and Mobile Computing (IWCMC'07), NewYork, USA, 12-15 Aug, pp. 388-392, 2007.

[17] Y.Zhou and Y.Fang,"BABRA: Batch-Based Broadcast Authentication in Wireless Sensor Networks," In Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'06), San Francisco, California, USA, 27 Nov-1 Dec, pp. 1-5, 2006.

[18] Y. Jiang, C. Lin, X. Shen, and M. Shi,"Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks," IEEE Transactions on Wireless Communications, Vol. 5, No. 9, pp. 2569–2576, Sep 2006.

[19] Yanjiang Yang,"A Practical Password-Based Two Server Authentication and key Exchange System," IEEE Transactions on Dependable and Secure Computing, Vol. 3, No. 2, pp. 105-114, Apr-Jun 2006.

[20] Qing Li,"Reducing delay and enhancing DoS resistance in Multicast Authentication through Multigrade Security," IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, pp.190-204, Jun 2006.

[21] Jianmin Zhang and Xiande Liu,"An Efficient Scheme for Broadcast Authentication in Wireless Sensor Networks," 1st International Conference on Communications and Networking, Beijing, China, 25-27 Oct, pp. 1-3, 2006.

[22] S.Choi,"Denial-of-Service Resistant Multicast Authentication Protocol with Prediction Hashing and One-Way Key Chain," In Proceedings of 7th IEEE International Symposium on Multimedia, CA,USA, 12-14 Dec, pp. 701-706, 2005.

[23] Wen Huei Chen,"A Bootstrapping Scheme for Inter-Sensor Authentication within Sensor Networks," IEEE Communications Letters, Vol. 9, No. 10, pp. 945-947, Oct 2005.

[24] D. Boneh, E.-J. Goh and K. Nissim, "Evaluating 2-DNF Formulas on Ciphertexts", Theory of Cryptography, Lecture Notes in Computer Science 3378, pp. 325-341, Feb 2005.

[25] D. Liu, P. Ning, and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks,"ACM Transactions on Information and System Security (TISSEC), Vol. 8, No. 1, pp. 41-77, Feb 2005.

[26] Micah Sherr,"Mitigating DoS Attack Through Selective Bin Verification," IEEE International Conference on Network Protocols (ICNP) Workshop on Secure Network Protocols, Boston, Massachusetts, USA, Nov 6, pp. 7-12, 2005.

[27] C. Karlof, N. Sastry, Y. Li, A. Perrig, and J.D. Tygar, "Distillation Codes and Applications to DoS Resistant Multicast Authentication," In Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS'04), San Diego, California, 5-6 Feb, 2004.

[28] C. A. Gunter and S. Khanna,"Dos Protection for Reliably Authenticated Broadcast ," In Proceedings of 11th Annual Network and Distributed System Security Symposium (NDSS'04), San Diego, California, 5-6 Feb, 2004.

[29] S.Rafaeh and D.Hutchison,"A Survey of Key Management for Secure Group Communication," ACM Computing Surveys (CSUR), New York, USA, Vol. 35, No. 3, pp. 309-329, Sep 2003.