ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

An Efficient ID-Based Scheme For Filtering Gang Injected False Data In Wireless Sensor Networks

Anjali Thampi K.G[1], L.M. Nithya[2]

PG Scholar, IT Department, SNS College Of Technology, Coimbatore, India [1]
HOD, IT Department, SNS College Of Technology, Coimbatore, India[2]

Abstract: Wireless sensor networks are usually deployed at aggressive environments which are more vulnerable to various security attacks such as selective forwarding, wormholes and sybil attacks. In such network user authentication is essential in any service-oriented communication network in order to identify and reject any access request of an unauthorized user. This project of wireless sensor networks focus on injecting false data attack and their mitigation techniques. For an injecting false data attack, an attacker node first compromises the sensor nodes and then accesses all keying materials stored in the compromised nodes and then controls these compromised nodes to inject bogus information and send the false data to the sink to cause upper-level error decision as well as energy depletion in en-route nodes. Therefore filtering false data should also be executed as early as possible to mitigate the energy consumption. To tackle this challenging issue false data filtering mechanisms known as novel bandwidth-efficient cooperative authentication (BECAN) scheme is developed for filtering injected false data in wireless sensor networks. Although it identifies false data attack it cannot prevent gang injecting false data attack from mobile compromised sensor nodes. To enhance the efficiency of verification, a new ID-based signature scheme is proposed that allows batch verification of multiple signatures to mitigate gang injection of false attack threat. It allows any pair of users to communicate securely and to verify each other's signatures without exchanging public key certificates.

Keywords: Filtering false data, En-route Filtering, BECAN,ID-Based Scheme, DSS Signature, compromised nodes, Gang injection
.

I. INTRODUCTION

A wireless sensor network is usually composed of a large number of sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. Each node is of low-cost and also equipped with sensing, da processing data, and communicating components. So, when a sensor node generates a report after being triggered by a special event.e.g, a while surrounding temperature change, it will send the report to sink through an established routing path. Such nodes are very vulnerable to various security attacks such as selective forwarding, wormholes attacks. In addition, wireless sensor networks also suffer from injecting bogus data attack.

For an injecting false data attack, an attacker node first compromises several sensor nodes and accesses all keying materials stored in the compromised nodes then controls these compromised nodes to inject false information and send those data to the sink to cause upper-level error decision. Therefore, it is crucial to filter the false data as accurately as possible in wireless sensor networks which results in energy deprivation. To tackle this issue, some false data filtering mechanisms have been developed.

Prior Filtering mechanisms use the symmetric key technique when the node is compromised. Those can abuse its keys to generate false reports and the reliability of the filtering mechanisms is degraded which makes hard to identify the node. Ye et al. propose a statistical en-routing filtering Mechanism called SEF. It requires each sensing report be validated by multiple keyed message authenticated (MACs). Each generated by a node detects the same event. As the report is forwarded, each node along the way verifies the correction of the MACs at earliest point. If the injected false data escapes the en-routing filtering nodes and then delivered to the sink to verify the correctness of each MAC carried in each report and reject false datas. In SEF, to verify the correctness of MACs, each node will get a random subset of the keys of size k from the global key pool of size N and uses them to producing the MACs. To save the bandwidth, SEF adopts the bloom filter to reduce the MAC size. SEF does not consider the possibility of compromise nodes which is crucial to the false data filtering.

Zhu et al. present an interleaved hop-by-hop authentication (IHA) scheme for filtering of injected false data. In IHA, each node is associated with two other nodes along the path, one is the lower association node and the other is the upper association node. An en-routing node will forward receive report if it is successfully verified by its lower association node. To reduce the size of the report, the scheme compresses individual MACs by XOR-ing them to one. However, the security of the scheme is mainly subject upon the creation of associations in the association discovery phase. Once the creation fails, the security cannot be guaranteed.

Location-Based Resilient Secrecy (LBRS), adopts location key binding mechanism to reduce the damage caused by node compromise, and further mitigates the false data generation in wireless sensor networks. It propose location-aware end-to-end data security design (LEDS) to provide end-to-end security guarantee including efficient en-routing false data filtering capability and high-level assurance on data availability. Because these LEDS are a symmetric key based solution, to achieve an en-routing filtering, it requires location-aware key management, where each node should share at least one authentication key with one node in its upstream/downstream report.

Zhang et al. provides a public key based solution to the same problem. Especially, they propose the notion of location-based keys by binding the private keys of individual nodes to both their IDs and geographic locations and a suite of location-based compromise-tolerant security mechanisms. To achieve en-routing filtering, additional 20 bytes authentication overheads are required.

Bit-compressed authentication technology achieves bandwidth-efficiency. Canetti et al. use one-bit authentication to achieve multicast security. The basic idea in multicast is very similar to the BECAN scheme, where a source knows a set of keys, each recipient knows a subset of them. When the source sends a message M, it authenticates M with each of the keys using MAC. Each recipient verifies MACs which were created using the keys in its subset. If any of these MACs is incorrect, the message M will be rejected. To achieve the bandwidth efficiency, each MAC is compressed as single bit. The security of the scheme is based on the assumption that the source is not compromised. However, once the source is compromised the scheme obviously does not work. Therefore, it cannot be applied to filter false data injected by compromised nodes.

A.Applications

1. In Public WLAN provides campus-wide indoor and outdoor coverage.
2. It provides flexible solution to implement the information delivery system required to control transportation services.
3. Wildlife monitoring focuses on tracking wild species to deeply investigate their behaviour and understand the interactions and influences on each other, as well as their reaction to the ecosystem changes caused by human activities.
4. Opportunistic networks can provide intermittent Internet connectivity to rural and developing areas where they typically represent the only affordable way to help bridging the digital divide.
5. VANETs use ad hoc communications for performing efficient driver assistance and car safety. The communications include data from the roadside and from other cars. VANET research aims to supply drivers with information regarding obstacles on the road and emergency events, mainly due to line-of-sight limitations and large processing delays. VANET can be used to communicate premonitions, notification of emergencies, and warnings about traffic conditions.
6. The underwater wireless sensor network have applications including the scientific (e.g., oceanographic data collection for scientific exploration, pollution control, or climate monitoring), military (e.g., tactical surveillance), and civilian fields (e.g., tsunami warnings).

II.NETWORK MODEL

Consider a typical wireless sensor network which consists of a sink and a large number of sensor nodes
N ={N0;N1} randomly deployed at a certain interest region (CIR) with the area S. The sink is a trustable and powerful data collection device, which has sufficient computation and storage capabilities and is responsible for initializing the sensor nodes and collecting the data sensed by these nodes. Each sensor node Ni ϵ N is stationary in a location.
For differentiation purpose, we assume each sensor node has a unique nonzero identifier. The communication is bidirectional, i.e., two sensor nodes within their wireless transmission range (R) may communicate with each other. Therefore, if a sensor node is close to the sink, it can directly contact the sink. However, if a sensor node is far from the transmission range of the sink, it should resort to other nodes to establish a route and then communicate with the sink. Formally, such a wireless sensor network, as shown in Fig. 1.1.1, can be represented as an undirected graph G = (v,ε) where V = (v1; v2; . . .) is the set of all sensorsN =(N0;N1; . . .) plus the sink, and ε=((vi; vj)|vi; vj ϵ V) is the set of edges.

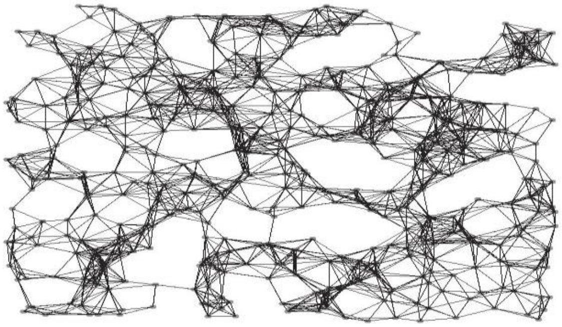


Fig 1. Network Model of WSN

III. LITERATURE REVIEW

A.KeyManagement Scheme

Distributed Sensor Networks (DSNs) are being widely used in many applications such as real-time traffic monitoring, military sensing and tracking, wildlife monitoring and tracking, etc. DSNs are ad-hoc mobile networks that may include thousand of sensor nodes with limited computation and communications capabilities. DSN topology can be dynamic and allow addition and deletion of sensor nodes after deployment. Besides, they may be deployed in hostile areas and hence the sensor nodes can be vulnerable to attacks by the adversaries. Because of the limited computation and communication capabilities of the sensor nodes, it is difficult to bootstrap the establishment of a secure communications infrastructure from a collection of sensor nodes which may have been pre-initialized with some secret information but have had no prior direct contact with each other.

Although prior schemes suggested the use of the random keys to establish the secure connections between the nodes, the idea of different security needs for different locations of nodes is not considered. Besides, the limited key pool will be eventually used up if the number of nodes grows dramatically. The scalability of random key predistribution is a concern and was left unaddressed in the basic and q-composite schemes

1.Issues in existing system

To address the bootstrapping problem in DSNs, Eschenauer et al firstly proposed the random key predistribution scheme that relies on probabilistic key sharing among the nodes of a DSN and uses simple protocols for shared key discovery and path key establishment. The basic idea is that a random pool of keys is selected from the key space. Each sensor node then receives a random subset of keys from the key pool before deployment. Any two nodes able to find a common key within their respective subsets can use that key as their shared secret to initiate communication and to set up the secure connection to identify connection setup process

2.Advantages of proposed system

The cluster based hierarchical topology not only isolates the effect of node compromise into one specific subgroup and provides scalability for node and subgroup addition, but more importantly, it simplifies the design of key management scheme for the sensor networks.

B.Effective Multiuser Broadcast Authentication

Wireless Sensor Networks (WSNs) have enabled data gathering from a vast geographical region and present unprecedented opportunities for a wide range of tracking and monitoring applications from both civilian and military domains. In these applications, WSNs are expected to process, store, and provide the sensed data to the network users upon their demands. As the most common communication paradigm, the network users are expected to issue the queries to the network in order to obtain the information of their interest. Furthermore in wireless sensor and actuator networks, the network users may need to issue their commands to the network

1.Issues in existing system

Digital Signature

A digital signature algorithm is a cryptographic tool for generating non repudiation evidence, authenticating the integrity as well as the origin of a signed message. In a digital signature algorithm, a signer keeps a private key secret and publishes the corresponding public key. The private key is used by the signer to generate digital signatures on messages and the public key is used by anyone to verify signatures on messages.

The Direct Storage Based Authentication Scheme (DAS)

One way to reduce the message overhead and the computational cost is to eliminate the existence of the certificate. A straightforward approach is then to let sensor nodes simply store all the current users' ID information and their corresponding public keys.

2.Advantages of proposed system

- Reduces the Probability of a False Positive
- Using "Fast Forward, Slow React" Public Key Forgery Attacks is prevented

IV. BECAN SCHEME

A novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data is deployed in existing system. Based on the random graph characteristics of sensor node deployment and estimate the probability of k-neighbours which provides the necessary condition for cooperative bit-compressed BECAN authentication technique. This scheme saves energy by early detecting and filtering the majority of injected false data with minor extra overheads at the en-route nodes. In addition, only a very small fraction of injected false data needs to be checked by the sink which largely reduces the burden of the sink.

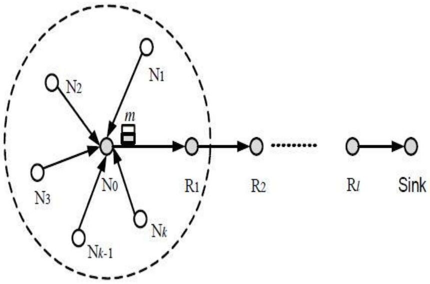


Fig 2 Architecture Of Existing System

The sink is a powerful data collection device. Nevertheless, if all authentication tasks are fulfilled at the sink, it is undoubted that the sink becomes a bottleneck. At the same time, if too much injected false data floods into the sink, the sink will surely suffer from the Denial of Service (DoS) attack. Therefore, it is critical to share the authentication tasks with the en-route sensor nodes such that the injected false data can be detected and discarded early. The earlier the injected false data is detected, the more energy can be saved in the whole network.

Achieving Bandwidth-Efficient Authentication Since the sensor nodes are low-cost and energy constraint, it is desirable to design a bandwidth efficient authentication scheme. For the BECAN scheme, once a compromised sensor node participates in the report confirmation, the report will be polluted and cannot reach the sink. To improve the reliability, multireports solution is naturally introduced in the BECAN scheme. As soon as critical tevent occurs, multisource nodes close to the event independently choose k different neighbours, produce the multi reports and send them to the sink via different paths. Only if one report reaches the sink, the true event will successfully reported. As a result, the reliability of the BECAN scheme can be improved

A.Disadvantages Of Becan Scheme

1. **Reliability**: If at least one report reaches the sink, the true event will successfully report else BECAN scheme cannot filter injected false data.
2. **Scalability:**
In the BECAN scheme, the additional authentication bits are in linear with the length of the path L. If L is too long, the authentication bits become large.
3. **BECAN** scheme is efficient for injecting false data by single attackers but not in case of group attackers.

B. Problem Definition

In the existing system the main problem is efficiency is low. And gang injection of false data could not be filtered and verified. A new stronger injecting false data attack, called gang injecting false data attack, in wireless sensor networks. This kind of attack is usually launched by a gang of compromised sensor nodes controlled and moved by an adversary A. As shown in Fig. 3, when a compromised source node is ready to send a false data, several compromised nodes will first move and aggregate at the source node, and then collude to inject the false data. Because of the mobility, the gang injecting false data attack is more challenging and hard to resist.

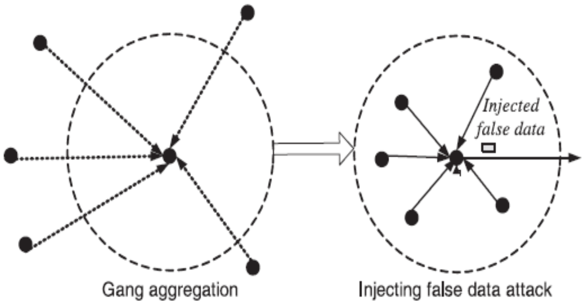


Fig.3 Gang Injection of false data

This kind of attack is usually launched by a gang of compromised sensor nodes controlled and moved by an adversary *A*. As shown in Fig. 2, when a compromised source node is ready to send a false data, several compromised nodes will first move and aggregate at the source node, and then collude to inject the false data. Because of the mobility, the gang injecting false data attack is more challenging and hard to resist.

V. ID BASED SCHEME

An identity (ID)-based signature scheme allows any pair of users to communicate securely and to verify each other’s signatures without exchanging public key certificates. The proposed new ID based signature scheme that allows batch verification of multiple signatures.
Using the new scheme, the signature size is reduced into almost half and efficiently verify multiple signatures. The verification cost of k signatures by a single signer is one signature verification plus k elliptic curve addition and k hashing. When a new signature by a different signer is added, additional verification cost is almost a half of that of ordinary verification of a single signature with minimal security loss.If there is an attacker who can forge a set of signatures to pass batch verification, then the computational Diffie-Hellman problem (CDHP) is used to solve such problem. Batch verification was devised to improve the efficiency of verification process for multiple signatures.

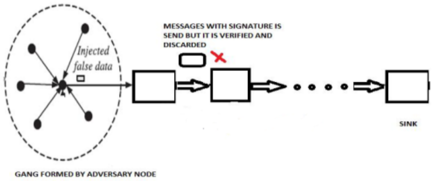

MESSAGES WITH SIGNATURE IS SEND BUT IT IS VERIFIED AND DISCARDED
Injected false data
SINK
GANG FORMED BY ADVERSARY NODE

Fig:4 ID Based Scheme

In the above figure ,it explains that the adversarial node form a gang. And these gang will inject false datas to the enroute nodes. Those enrote nodes will check whether the digitsl signatur in the report is correct or not. If its not correct then the report will be rejected or else it will be forwarded to the enroute nodes.

A.Advantages Of Proposed System

ID-based signature scheme is more secure and deploys an efficient batch verification.Aggregated Signature is a generalized version of Batch Signature where many signatures for different messages signed by different signers are aggregated into one signature and verified by one equation. Gang injecting false data is identified within limited time efficiently.

VI.MODULE DESCRIPTION

A.Sensor Nodes Initialization and Deployment

The sink first chooses an elliptic curve which selects a secure cryptographic hash function. The sink deploys these initialized sensor nodes at a certain interest region (CIR) in various ways such as by air or by land. But assume that all sensor nodes are uniformly distributed. When these sensor nodes are not occupied by the reporting task, they cooperatively establish their routing to the sink either a shortest path or a path adapted to some resource constrains with some existing routing protocol which accelerates the reporting. Once an event occurs, a report can be immediately relayed along the established routing path.

Algorithm 1. Sensor Nodes Initialization Algorithm

```
Procedure SENSORNODESINITIALIZATION
    Input: $params$ and un-initialized $\mathcal{N} = \{N_0, N_1, N_2, \ldots\}$
    Output: initialized $\mathcal{N} = \{N_0, N_1, N_2, \ldots\}$
    for each sensor node $N_i \in \mathcal{N}$ do
        preload $N_i$ with TinyECC, $params$ and energy
        choose a random number $x_i \in \mathbb{Z}_q^*$ as the private
        key, compute the public key $Y_i = x_i G$, and install
        $(Y_i, x_i)$ in $N_i$
    end for
    return initialized $\mathcal{N} = \{N_0, N_1, N_2, \ldots, N_n\}$
end procedure
```

B.Sensed Results Reporting Protocol

When a sensor node generates a report after being triggered by a special event or response to a query from the sink, it will send the report to the sink via established routing.

Algorithm 2. CNR Based MAC Generation

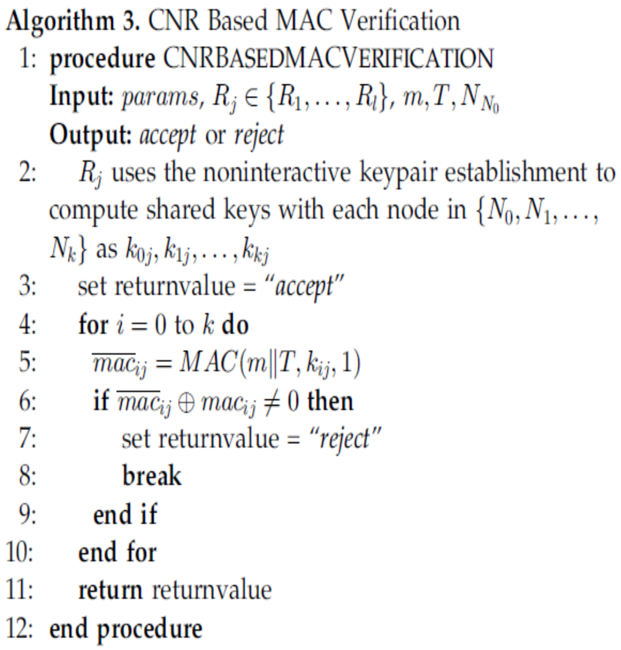
```
procedure CNRBASEDMACGENERATION
    Input: $params$, $N_i \in (N_{N_0} \cup N_0)$, $m, T, R_{N_0}$
    Output: $Row_i$
    $N_i$ uses the non-interactive keypair establishment to
    compute shared keys with each node in $R_{N_0}$ : $[R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_l \rightarrow Sink]$ as $k_{i1}, k_{i2}, \ldots, k_{il}, k_{is}$, where $k_{is}$
    is $N_i$'s private key distributed by the $sink$
    if $N_i$ believes the report $m$ is true then    ▷
    a neighboring node is assumed having the same ability
    to detect a true event as the source node and correctly
    judge the report $m$.
        for $j = 1$ to $l$ do
            $mac_{ij} = MAC(m \| T, k_{ij}, 1)$
        end for
        $mac_{is} = MAC(m \| T, k_{is}, \alpha)$
    else
        for $j = 1$ to $l$ do
            $mac_{ij}$ is set as a random bit
        end for
        $mac_{is}$ is set as a random bit string of length $\alpha$
    end if
    return $Row_i = (mac_{i1}, mac_{i2}, \ldots, mac_{il}, mac_{is})$
end procedure
```

C .En-Routing Filtering

The source node N0 gains the current timestamp T, chooses k neighboring nodes and sends the event and routing path. Each sensor node invokes the Algorithm 2 to generate a row authentication vector

$$Row_i = (mac_{i1}, mac_{i2}, \ldots, mac_{il}, mac_{is})$$

When each sensor node along the routing receives the message (m, T, MAC) from its upstream node, it checks the integrity of the message m and the timestamp T. If the timestamp T is out of date, the message (m, T, MAC) will be discarded. Otherwise, Ri invokes the Algorithm called cooperative neighbor router (CNR) MAC verification. If the returned value is “accept” Ri will forward the message (m, T, MAC) to its downstream node, Otherwise discard.



Algorithm 3. CNR Based MAC Verification

```
procedure CNRBASEDMACVERIFICATION
Input: $params$, $R_j \in \{R_1, \ldots, R_l\}$, $m, T, N_{N_0}$
Output: $accept$ or $reject$
    $R_j$ uses the noninteractive keypair establishment to compute shared keys with each node in $\{N_0, N_1, \ldots, N_k\}$ as $k_{0j}, k_{1j}, \ldots, k_{kj}$
    set returnvalue = "accept"
    for $i = 0$ to $k$ do
        $\overline{mac}_{ij} = MAC(m\|T, k_{ij}, 1)$
        if $\overline{mac}_{ij} \oplus mac_{ij} \neq 0$ then
            set returnvalue = "reject"
            break
        end if
    end for
    return returnvalue
end procedure
```

D. ID-based Batch Signature

This scheme consists of four algorithms: Setup, Extract, Signing and Verification.
Setup
Given a GDH group G and its generator P, pick a random s ∈ Z/`Z and set Ppub = sP. Choose two hash functions H1 : {0, 1}∗ × G → (Z/`Z)∗ and H2 :{0, 1}∗ → G∗. The system parameter is (P, Ppub,H1,H2). The master key is s.

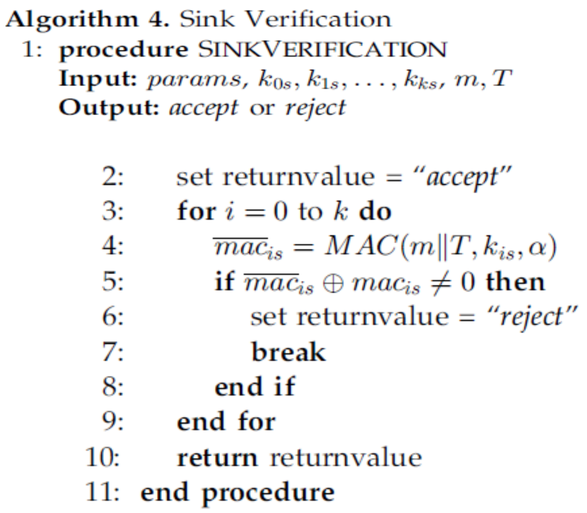
1.Extract
Given an identity ID, the algorithm computes QID = H2(ID) and DID =sH2(ID) and outputs DID as a private key of the identity ID corresponding to QID = H2(ID).

2.Signing
Given a secret key DID and a message m, pick a random number r ∈ Z/`Z and output a signature σ = (U, V) where U = rP, h = H1(m,U), and V = rQID+hDID.
3.Verification
Given a signature σ = (U, V) of a message m for an identity ID, compute h = H1(m,U). The signature is accepted if and only if (P,QID,U + hPpub, V) is a valid Diffie-Hellman tuple

4.Aggregate Verification
A forger is given a target public key for which a forged signature should be made. While each secret key of users is chosen independently in the traditional public key system, all secret keys of users are mutually related in ID-based system. In fact, they are produced from one secret key of the whole system. Hence in ID-based setting it is reasonable not to give specific ID but a system parameter to a forger.

5.K-aggregate forger of a chosen ID:
A forger succeeds if he can produce a set of k signatures which pass the aggregate verification. This type of forger is known as k-aggregate forger of a chosen ID.
6.K-aggregate forger of a given ID:
A forger produces a set of k signatures one of which has the signer with the given ID, then this type of forger is called a k-aggregate forger of a given ID.

E. Sink Verification
If the sink receives the report (m, T, MAC), it checks the integrity of the message m and the timestamp T. If the timestamp is out of date, the report (m, T, MAC) will be immediately discarded. Otherwise, the sink looks up all private keys and invokes Sink verification Algorithm. If the returned value of Algorithm is "accept," the sink accepts. Otherwise rejects the report.



Algorithm 4. Sink Verification

```
procedure SINKVERIFICATION
Input: $params$, $k_{0s}, k_{1s}, \ldots, k_{ks}$, $m, T$
Output: $accept$ or $reject$

    set returnvalue = "accept"
    for $i = 0$ to $k$ do
        $\overline{mac}_{is} = MAC(m\|T, k_{is}, \alpha)$
        if $\overline{mac}_{is} \oplus mac_{is} \neq 0$ then
            set returnvalue = "reject"
            break
        end if
    end for
    return returnvalue
end procedure
```

VI. RESULT

Filtering the false injected data is the main problem in wireless sensor network.The BECAN scheme is used to filter the false data by verifying the unique MAC of every node. These BECAN scheme is not so efficient to filter the data, it is time consuming and also the filtering ratio is much reduced. These BECAN scheme does not filter the gang injected false data .Thus the BECAN scheme is not so efficient so a scheme is introduced to filter the gang injected false data. These scheme is the ID-Based scheme.The ID-Based scheme is more efficient than other schemes.

The ID-Based signature scheme provides better results than the BECAN scheme. Here the signatures are verified. First the nodes are initialized in CIR region. When a sensor node generates a report m after being triggered by a special event, then it send the report to the sink via an established routing.

Then the signatures of every nodes are created and while reporting the task each and every signature is verified effectively. These signatures are verified by reducing the size of the signature. Thus when filtering the data the filtering rate is increased and also these are time consuming scheme. These scheme will filter the gang injected false data.

VII. COMPARISON GRAPH

The filtering ratio of two schemes are also compared.In the BECAN scheme the filtering ratio is not so efficient while compared with the ID Based scheme. In the ID based signature scheme the filtering ratio of the false datas are increased and they are efficient scheme than the BECAN scheme. In BECAN scheme the filtering ratio is 55% while in the ID Based scheme the Ratio is improved to 95%.

Because of the efficiency in the filtering the ID based scheme is used to filter the gang injected false data. In filtering the Gang injected False data the ID Based Scheme has a better result.

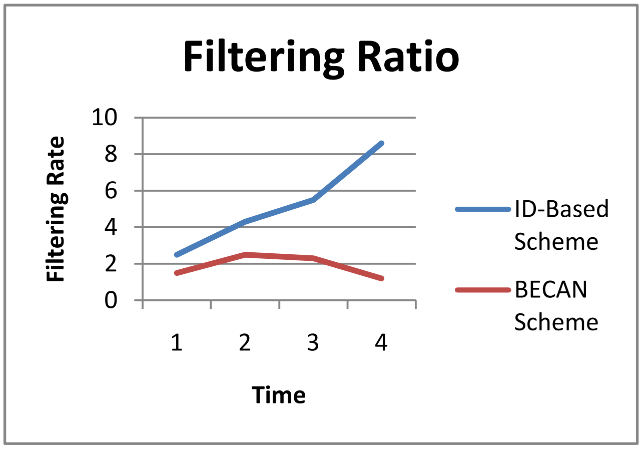


Fig 5. Comparison Graph

VIII. CONCLUSION AND FUTURE WORK

The BECAN scheme achieves not only high en-routing filtering probability but also high reliability for filtering the injected false data with multi-reports. Due to the simplicity and effectiveness, the BECAN scheme could be applied to other fast and distributed authentication scenarios in wireless mesh network. The existing scheme is further extended to mitigate gang injecting false data attack from mobile compromised sensor nodes using proposed ID-based signature scheme for efficient batch verification. Thus it verifies many signatures at the cost of almost one signature verification. If a signature by a different signer is added, the additional cost is a half of the single verification.

The future enhancement may be further aimed at improving the performance of proposed framework in terms of packet delivery ratio, end-to-end delay, as well as bandwidth efficiency with minimal energy consumption.

REFERENCES

[1]Akylidz.J,Weilian Su,Boyen.X (2003)"A Survey on Wireless Sensor Networks". IEEE Communication Magazine 2002 , LNCS, Vol. 2729, pp. 383399, Springer-Verlag,.

[2]Boyd.C, Mao.W, and Paterson.K.G, (2004) "Key Agreement Using Statically Keyed Authenticators," Proc. Second Int'l Conf. Applied Cryptography and Network C(ACNS '04), pp. 248-262.

[3]Black.J and Rogaway.J, (2005)"Cbc Macs for Arbitrary-Length Messages: the Three-Key Constructions," J. Cryptology, vol. 18, no. 2, pp. 111-131

[4]Cha .Jand Cheon. J,(2003)"An ID-based signature from gap-Diffe-Hellman groups. Public Key Cryptography"- PKC 2003, LNCS Vol. 2567, Springer- Verlag.

[5]Chen.J, Yu.Q, Zhang.Y, Chen.H, and Sun.Y, (2010)"Feedback Based Clock Synchronization in Wireless Sensor Networks: A Control Theoretic Approach," IEEE Trans. Vehicular Technology, vol. 59, no. 6, pp. 2963-2973. [6]Dong.J, Chen.Q, and Niu.Z, (2007)"Random Graph Theory Based Connectivity Analysis in Wireless Sensor Networks with Rayleigh Fading Channels," Proc. Asia- Pacific Conf. Comm. (APCC '07),pp. 123-126.

[7]Eschenauer.L and Gligor.V.D, (2002)"A Key-Management Scheme for Distributed
Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS'02).

[8]Giruka.V.C, Singhal.M, Royalty.Y, and Varanasi.S, (2007)"Security in Wireless Sensor Networks," Wireless Comm. and Mobile Computing,vol. 8, no. 1, pp. 1-24. [9]Hankerson.D, Hernandez.Jand Menezes (2006) "A Software Implementation of Elliptic Curve Cryptography Over Binary Fields. Proc. of CHES 2000, LNCS, Vol. 1965, Springer-Verlag.

[10]Lu.R, Lin.X, Zhang.C, Zhu.H, Ho.P, and Shen.X, (2008)"AICN: An Efficient Algorithm to Identify Compromised Nodes in Wireless Sensor Network," Proc. IEEE Int'l Conf. Comm. (ICC '08).

[11]Lin.X, Lu.R, and Shen.R, (2010)"MDPA: Multidimensional Privacy-Preserving Aggregation Scheme for Wireless Sensor Networks," Wireless Comm. and Mobile Computing, vol. 10, pp. 843-856.

[12]Lin.X, (2007)"CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks," Proc. IEEE GLOBECOM '09.

[13]Li.X,Santoro.N, and Stojmenovic.I, (2008)"Localized Distance-Sensitive Service Discovery in Wireless Sensor and Actor Networks," IEEE Trans. Computers, vol. 58, no. 9, pp. 1275-1288.

[14]Li.X, Nayak.A, Simplot-Ryl.A, and Stojmenovic.I,(2010) "Sensor Placement in Sensor and Actuator Networks," Wireless Sensor and Actuator Networks: Algorithms and Protocols for Scalable Coordinationand Data Communication, Wiley.

[15]Ren.K, Lou.W, and .Y.Zhang,(2007) "Multi-User Broadcast Authentication in
Wireless Sensor Networks," Proc. IEEE Sensor Ad Hoc Comm. Networks (SECON'07), June.

[16]Ren.K, Lou.W, and Zhang.Y,(2006) "LEDS: Providing Location-Aware End-to- End Data Security in Wireless Sensor Networks," Proc. IEEE INFOCOM '06.. [17]Szewczky.R, Mainwaring.A, Anderson.J, and Culler.D, (2004)"An Analysis of a Large Scale Habit Monitoring Application," Proc. Second ACM Int'l Conf. EmbeddeNetworked Sensor Systems (Sensys '04).

[18] Xiaodong Lin, Rongxing Lu, Pin-Han Ho, Xuemin (Sherman) Shen, (2008)"TUA: A Novel Compromise-Resilient Authentication Architecture forWireless Mesh Networks" IEEE transactions on wireless communications, vol.7, no. 4. [19]Yang.H, Ye.F, Yuan.Y, Lu.S, and Arbaugh.W,(2005) "Toward Resilient Security in Wireless Sensor

Networks," In ACM Proceedings of MobiHoc pp.34-45.
[20]Ye.H, Luo.H, Lu.S, and Zhang.L, (2004)"Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM '04.. [21]Yu.C.M, Lu.C.S, and Kuo S.Y, (2005)"A Dos-Resilient En-Route Filtering Scheme for Sensor Networks," Proc. Tenth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '09), pp. 343-344.
[22]Zhang.C, Lu.R, Lin.X, Ho.P, and Shen.X, (2008)"An Efficient Identity- Based
Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM'08.
[23]Zhou.L and Ravishankar.C, (2005)"A Fault Localized Scheme for False Report
Filtering in Sensor Networks," Proc. Int'l Conf. Pervasive Services, (ICPS '05), pp.59-68.
[24]Zhu.Z, Tan.Q, and Zhu.P, (2007)"An Effective Secure Routing for False Data Injection Attack in Wireless Sensor Network," Proc. 10th Asia-Pacific Network Operations and Management Symp. (APNOMS '07), pp. 457-465.
[25]Zhu.S, Setia.S, Jajodia.S, and Ning.P,(2004) "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy.
[26] Zhu.S, Setia.S (2009)" STEF: A Secure Ticket-Based En-route FilteringScheme for Wireless Sensor Networks" Proc. 10th Asia-Pacific Network Operations and Management Symp. (APNOMS '07), pp. 457-465