BANDWIDTH EFFICIENT COOPERATIVE AND ENERGY BASED AUTHENTICATION FOR WIRELESS SENSOR NETWORK

A.P.THANGAMUTHU[1], B.CHITHRA[2]

[1] Asst Prof, Department of Computer Applications, SNMV College of Arts and Science, Tamil Nadu, India
[2]Asst Pof, Department of ComputerTechnology, SNMV College of Arts and Science, Tamil Nadu, India

Abstract - Wireless detector networks (WSNs), as associate degree rising technology face varied challenges. Detector nodes are typically resource constrained and conjointly at risk of physical attacks or node compromises. Because the projected applications for wireless detector networks vary from sensible applications like traffic monitoring to important military applications like menstruation levels of gas concentration in battle fields, security in detector networks becomes a first-rate concern. In sensitive applications, it becomes imperative to unceasingly monitor the transient state of the system instead of steady state observations and take requisite preventive and corrective actions.

This paper propose a bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data in Wireless sensor Networks. Sensor node could be easily compromised as the attacker can gain control obtain key values and change the properties of the node. This results in a false report to sink and energy waste in end-route nodes. The proposed BECAN scheme can save energy by early detecting and filtering the most of injected false data with less time and difficulty at the en-route nodes. In addition, only a very small amount of injected false data needs to be checked by the sink, thereby reducing the burden on sink. To filter the false data, the BECAN scheme adopts cooperative neighbor router (CNR)-based filtering mechanism. Hence it achieves not only high filtering probability but also high reliability.

1. INTRODUCTION

Wireless sensor networks are usually deployed at unattended or hostile environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, wormholes, and Sybil attacks. In addition, wireless sensor networks may also suffer from injecting false data attack. For an injecting false data attack, an adversary first compromises several sensor nodes, 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 wasted in en-route nodes.

The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Wireless sensor networks (WSN) offer an increasingly Sensor nodes need less power for processing as compared to transmitting data. It is preferable to do in network processing inside network and reduce packet size. One such approach is data aggregation.

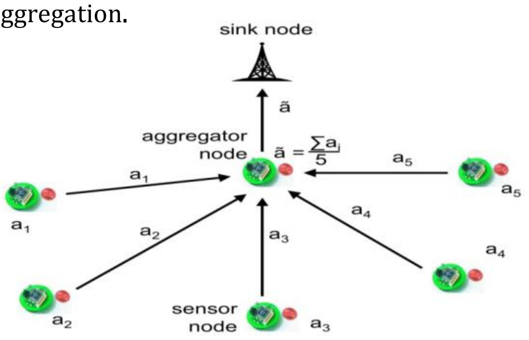


Fig. 1 Wireless Sensor Network Architecture.

Wireless sensor networks are consisting of numerous light weight and tiny sensor nodes with limited power, storage, communication and computation capabilities.

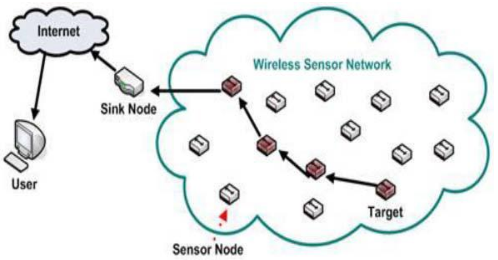


Fig 2. Data transmitted user to target

Due to the fast booming of micro electro mechanical systems, wireless sensor et working has been subject to extensive research efforts in recent years. It is well known as a general and ubiquitous approach for some applications like environmental and habitat monitoring, surveillance and tracking for military [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16]. 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. The cost of each sensor node is low but it contains required sensing, communicating and data processing components. Deployment of wireless sensor networks is usually done at adverse or unaccompanied environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, wormholes, and Sybil attacks [12], [18].

We 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. Sink is liable for initializing the sensor nodes and collecting data by these sensor nodes and sink is considered to be powerful and trustable data collection device, since it has enough storage and computational capabilities.

Let v1 denote the sink. All sensor nodes can run the Dijkstra shortest path algorithm (see Appendix) to find their shortest paths to the sink v1, only if the graph is fully connected. Probability of fully connected. Assume that the positions of these vertexes V = {v1, v2, . . .} are uniformly distributed in the area S with network. Density where, and |V| denotes the cardinality of V. Based on the random graph theory, the probability that there are n nodes in an arbitrary region A with the area A is,

$$P(N = n|A)$$
$$= \binom{|V|}{n}\binom{\pi.A}{|V|} pow\ (n).\left(-\frac{\pi.A}{|V|}\right) pow(|V| - n)$$
$$= \binom{|V|}{n}\left(\frac{A}{S}\right) pow(n).\left(1 - \frac{A}{S}\right) pow(|V| - n)$$

To calculate the full connection probability Pcon, we first compute Piso, the isolation probability of any node in G= {V, E}, where a node is called isolated if there exists no link among it and any other nodes. In other words, in some circle coverage with the area πR2, except one node lies at the center, no other node exists. Suppose the border effects are neglected Fig. shows the full connection probability Piso versus different transmission ranges R and |V|. It can be seen that the expected fully connected G= {V, E} can be achieved by choosing proper R and |V|.

1.1 Design Goal

The design goal is to develop an efficient cooperative bandwidth-efficient authentication scheme for filtering the injected false data. The two desirable objectives are as follows.

1.1.1 Premature detection of injected false data by En-Route Sensor Nodes

A bandwidth efficient authentication method has to be designed because costs of sensor node are low and energy constraint. The sink is said to be trustable and powerful data collection device. Undoubtedly, the sink will become a bottleneck if authentication is done at sink. Sink will also suffer from Denial of Service (DoS) attack if more injected false data comes into it. 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. If injected false data is detected at the earliest, then large energy will be saved in the entire network.

2. RELATED WORK

Recently, some research works on bandwidth-efficient filtering of injected false data in wireless sensor networks have been appeared in the literature in [9], [10], [11], [12], [13]. In [9], Ye et al. propose a statistical en-routing filtering mechanism called SEF. SEF requires that each sensing report be validated by multiple keyed message authenticated (MACs), each generated by a node that detects the same event. Early verification of MACs correctness along the path when report is being forwarded is done at every node.

In order to reduce MAC size and to save bandwidth, bloom filter is adopted by SEF. Within 10 hops SEF can prevent 80-90 percent probability of injected false data by simulation. However, since n should not be large enough as described above, the filtering probability at each en-routing node p = k(T-Nc)/N is relatively low. Besides, SEF does not consider the possibility of en-routing nodes' compromise, which is also crucial to the false data filtering. In [10], Zhu et al. present an interleaved hop-by-hop authentication (IHA) scheme for filtering of injected false data.

We have to analysis the Parallel and distributed systems Survey:

Parallel and distributed computing

1.“A distributed system is a collection of independent computers that appear to the users of the system as a single computer.”

2.“A distributed system consists of a collection of autonomous computers linked to a computer network and equipped with distributed system software.”

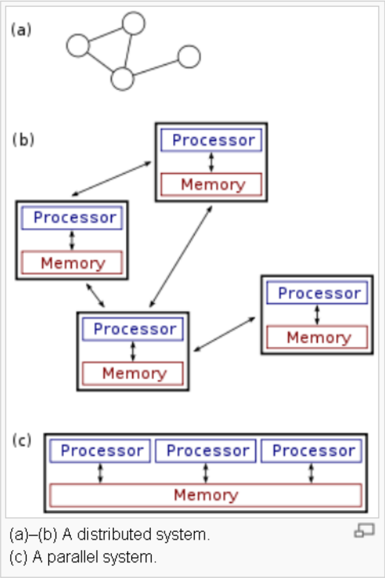
3.“A distributed system is a collection of processors that do not share memory or a clock.”

4.“Distributed systems are a term used to define a wide range of computer systems from a weakly-coupled system such as wide area networks, to very strongly coupled systems such as multiprocessor systems.”

Nevertheless, it is possible to roughly classify concurrent systems as "parallel" or "distributed" using the following criteria:

•In parallel computing, all processors have access to a shared memory. Shared memory can be used to exchange information between processors.

• In distributed computing, each processor has its own private memory (distributed memory). Information is exchanged by passing messages between the processors.



(a)–(b) A distributed system.
(c) A parallel system.

Fig 3 Processing Of Data Momery Allacation

The figure on the right illustrates the difference between distributed and parallel systems. Figure (a) is a schematic view of a typical distributed system; as usual, the system is represented as a network topology in which each node is a computer and each line connecting the nodes is a communication link. Figure (b) shows the same distributed system in more detail: each computer has its own local memory, and information can be exchanged only by passing messages from one node to another by using the available communication links. Figure (c) shows a parallel system in which each processor has a direct access to a shared memory.

The situation is further complicated by the traditional uses of the terms parallel and distributed algorithm that do not quite match the above definitions of parallel and distributed systems.

Chan propose three mechanisms for sensor networks one mechanism uses a composite random key predistribution scheme. Any two sensor nodes want to establish a pair wise key. This scheme achieves high security in wireless sensor networks. Another one called Multipath key reinforcement scheme is a method to strengthen the security to set up a link key via Multipath. Let two sensor nodes P and Q want to set up a link key. Node P sends j different random values to node Q. These values are sent to Q along different paths. .The third mechanism uses a random pairwise key scheme. In this a unique random pairwise key is generated for a pair of nodes, and an ID for the node is created and also stored along with the key .Each node can find its shared common pair wise keys with its neighbors nodes using their node IDs.

In the paper “TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks” by Liu and Ning introduces two pair wise key predistribution schemes: First a random subset assignment scheme and second a grid-based key predistribution scheme. In the first one a server generates a set of tdegree polynomials. for which a unique ID is assigned. Each sensor node has a subset of these polynomials. Any two nodes that have same polynomial can set pairwise key between them directly. Others will use path key establishment method. A source node sends a request to its i forwarding nodes to establish a pair wise key with the destination node. This request will be forwarded until a node finds a path to the destination node. In the second scheme, the server assigns each enrooting node an ID and corresponding row and column polynomial. Two sensor nodes establish a pair wise key between them. If there is no match they will find a path with the help of forwarding nodes.

3. METHODOLOGY

In this paper, we propose a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data in wireless sensor networks. Compared with the previously reported mechanisms, the BECAN scheme achieves not only high filtering probability but also high reliability. The main contributions of this paper are threefold.

- First, we study the random graph characteristics of wireless sensor node deployment, and estimate the probability of k-neighbors, which provides the necessary condition for BECAN authentication;
- Second, we propose the BECAN scheme to filter the injected false data with cooperative bit-compressed authentication technique. With the proposed mechanism, injected false data can be early detected and filtered by the en-route sensor nodes. In addition, the accompanied authentication information is bandwidth-efficient; and
- Third, we develop a custom simulator to demonstrate the effectiveness of the proposed BECAN scheme in terms of en-routing filtering probability and false negative rate on true reports.

A. **Statistical En-route Filtering (SEF)** This mechanism uses Message Authenticated Code (MAC).In detection of an event each report generated by the sensor nodes validated by multiple keyed message authenticated code (MACs).

B. Interleaved hop-by-hop authentication (IHA) In this scheme the sensor node is associated with two other forwarding nodes along the path. The one closer to the base station is the upper associated node and the other is the lower associated node.

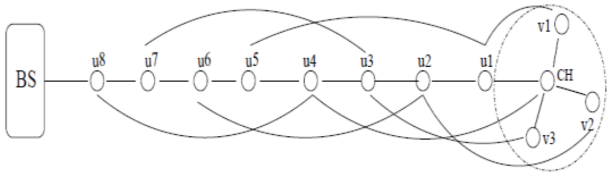


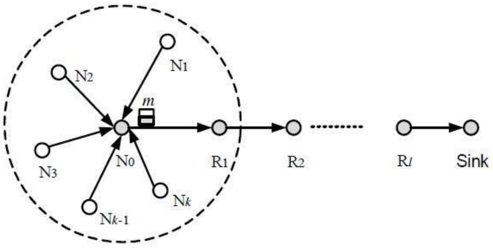
Fig 4 Data Clustering For Ach Node

C. Location-Based Resilient Secrecy (LBRS) This system adopts a location key binding mechanism. This will reduce the damage caused to node by an attacker and further reduces the false data generation in wireless sensor networks.

D. Location-aware end-to-end data security design (LEDS) This mechanism is provide end-to-end security efficient and high data availability. LEDS uses a symmetric key and location key management, to achieve high en-routing filtering.

E. Bit-compressed authentication Technology This technology can achieve bandwidth-efficient by compressing MAC single bit. This provides high security.

F. Limitations of Existing System In Statistical En-route Filtering (SEF), the filtering probability at each sensor node is relatively low. It detect maximum of injected false reports. But does not consider the possibility of en-routing sensor nodes compromise. In Interleaved hop-by-hop authentication (IHA), if creation of association fails, it is vulnerable to attack.IHA use the symmetric key for authentication, which allows the compromised nodes to misuse it to generate false reports



The design goal of proposed system is to achieve bandwidth-efficient authentication for filtering injected false data. Every sensor node in wireless sensor network shares a private key with the sink.Each node knows its one-hop neighbors and establish a public-private key pair with each of them. In this scheme it use Message Authentication Code (MAC) mechanism to authenticate broadcast messages and every node can verify the broadcast messages.Each MAC is set to 1 bit to achive bandwidth efficient authentication. To filter the false data injected by attacked sensor nodes, the BECAN scheme adopts cooperative neighbor router (CNR)-based filtering mechanismas in figure 2 .Here a source node N0 is ready to send a report m to the sink via an established routing path PN0: {P1 – P2 ...Pl – Sink}, it first resorts to its k neighboring sensor nodes SN0 : {S1,S2, . . .,Sk} to cooperatively authenticate the report m, and then sends it together with the authentication information MAC from N0 to the sink via routing RN0, where the sink initializes all sensor nodes, then each one of it shares its private key with the sink.

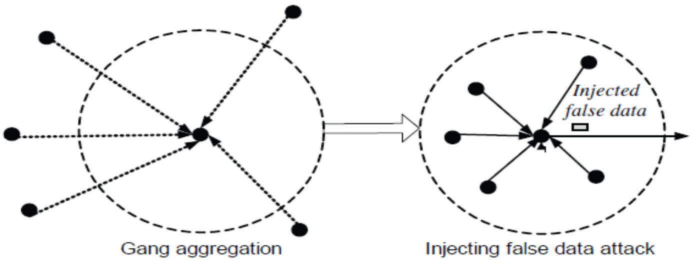


Fig 5. Data applying the Nodes

Description of BECAN Authentication

The BECAN authentication scheme consists of two phases: sensor nodes initialization and deployment, and sensed results reporting protocol.

Sensor Nodes Initialization and Deployment

Given the security parameter k, the sink first chooses an elliptic curve defined over IFp, where p is a large prime and function is a base point of prime order q with |q|=k. A secure cryptographic hash function h ( ) is then selected by sink, where h: {0, 1}*. Inally, the sink sets the public parameters as params = {E(IFp),G, q, h( )}.

En-Routing Filtering

When each sensor node Ri, (1 ≤ i ≤ l), along the routing RN0 receives (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. If the returned value is "accept," Ri will forward the message (m, T, MAC) to its downstream node, Otherwise, (m, T, MAC) will be discarded.

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 kis of Ni, 0 ≤ i ≤ k.

Fig 6. Data transmitted path and cluster

Reliability of the BECAN scheme. In addition to the high (en-routing) filtering probability, the BECAN scheme also has high reliability, i.e., even though some sensor nodes are compromised, the true event reports still can reach the sink with high probability,

Let FNR be the false negative rate on the true reports and tested as,

$$FNR = \frac{number\ of\ true\ data\ that\ cannot\ reach\ the\ sink}{total\ number\ of\ ture\ data}$$

If FNR is small, the BECAN scheme is demonstrated high reliability. FNR can be increased by selectively dropping true report attack [18]. However, its adverse impact can affect any routing algorithm. Thus, for fairness, we only consider FNR that caused by 1) the number of uncompromised neighboring sensor nodes being less than k, 2) Some compromised sensor nodes polluting the true report.

In this paper, we propose a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data. Based on the random graph characteristics of sensor node deployment and the cooperative bit-compressed authentication technique, the proposed BECAN scheme can save 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 thus largely reduces the burden of the sink. Both theoretical and simulation results are given to demonstrate the effectiveness of the proposed scheme in terms of high filtering probability and energy saving.

A.SENSOR NODE INITIALIZATION

In this technique, the key server generates unique public and private keys for each sensor node and sink. These keys will be shared to the sensor nodes when they start.

B.CNR BASED MAC GENERATION

This technique is used by the sensor nodes for generating authentication message. This technique uses Elliptic curve cryptography and DES algorithm.

C.CNR BASED MAC VERIFICATION

In this phase, the sink verifies the authentication message sent by sensor node using ECC algorithm.

D.SINK VERIFICATION

In this module, the sink verifies each message sent by sensor nodes weather it is valid or invalid.

E.ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

It is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Public-key cryptography is based on the intractability of certain mathematical problems.

F.DESIGN RATIONALE

To filter the false data injected by compromised sensor nodes, the BECAN adopts cooperative neighbor router (CNR) based filtering mechanism. As shown in Fig. 5 CNR-based mechanism, when a source node N0 is ready to send a report m to the sink via an established routing path RN0: [R1 -> R2 ->. . Rl-> Sink], it first resorts to its k neighboring nodes NN0: {N1, N2, . ..,Nk} to cooperatively authenticate the report m, and then sends the report m and the authentication information MAC from N0 U NN0 to the sink via routing RN0.

The following sections depict several practical design and implementation issues in building the proposed mechanism.

A. Sensor node initialization and deployment The base station (sink), forwarding node and sensor nodes has been designed The sink deploys these initialized sensor nodes at a Certain Interest Region (CIR).

B. Routing establishment

In the proposed model, base station, forwarding node and sensor nodes has been designed. Base station receives message from sensor node.

C. Sensed Results Reporting Protocol To filter the false data injected by compromised sensor nodes, the BECAN scheme adopts cooperative neighbor router (CNR)-based filtering mechanism. In the CNR-based mechanism, when a sensor (source) node N0 has sensed some data m and is ready to report m to the sink via the routing path RN0: {R1 - R2 …Rl – Sink}.

D. Filtering false injection attack when each sensor node Ri, along the routing RN0 receives message m, timestamp T, and MAC key from its upstream node, it checks the integrity of the message m and the timestamp T.

E. Sink Verification Sink receives report m, Timestamp and MAC. Check the time, if the timestamp is unmatched or old, then the report will be discarded. f one report reaches the sink correctly, it will be successfully reported. That's how reliability of the BECAN scheme improved.

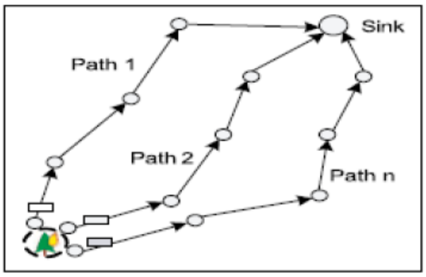


Fig 7 Data Path Selection Based Transmitting

BECAN Scheme also resolves the scalability problem. The devise a large sensor network is divided into a heterogenous sensor network .In each one consists of a powerful High-end sensor (Hsensor) acting as Cluster Head and a number of Low-end sensors (L-sensors), as shown in Fig. 4. L-sensor senses tevent send report to the neighboring H-sensor.

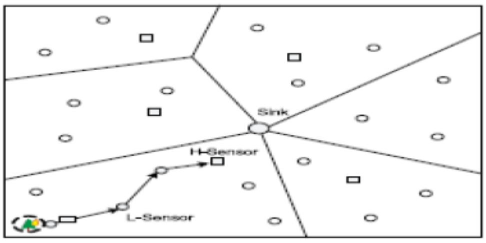
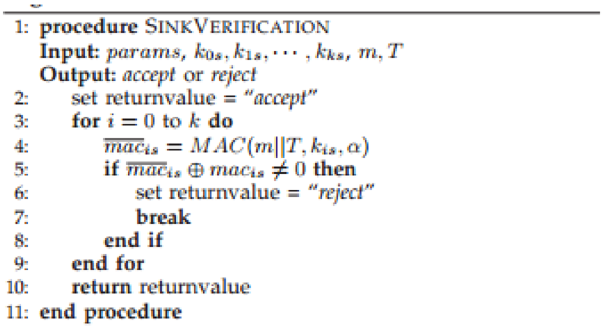


Fig 8. Clustering the data check sensor

Energy saving is always crucial for the lifetime of wireless sensor networks. In this section, the performance of the proposed BECAN scheme is evaluated in terms of energy efficiency.



```
procedure SINKVERIFICATION
Input: $params, k_{0s}, k_{1s}, \cdots, k_{ks}, m, T$
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
```

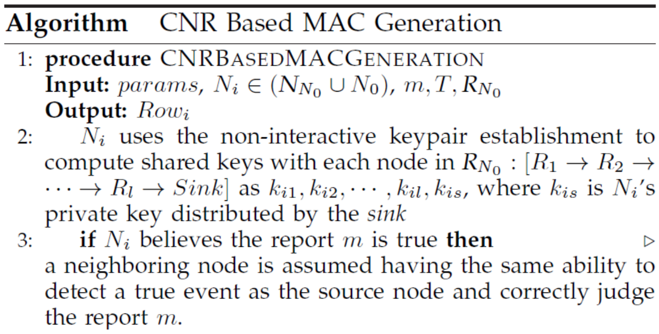
FIG 12 Energy Consumption in Non-interactive Key-pair Establishments

The proposed BECAN method has added computational cost because of expensive ECDH operations at the time of establishment of non-interactive key pair. Fortunately, since the non-interactive key pair establishments are averagely distributed in each sensor node and only executed once during the routing establishment, the ECDH operation is not a heavy burden. In order to achieve same amount of security as 1024 bit RSA,

Energy Consumption in Transmission

The majority of injected false data can be filtered by BECAN within 15 hops during transmission. Thus, BECAN can greatly save the energy of sensor nodes along the routing path.
Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.



```
Algorithm  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 $k_{i1}, k_{i2}, \cdots, k_{il}, k_{is}$, 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 $m$.
```

1. **BECAN Scheme**

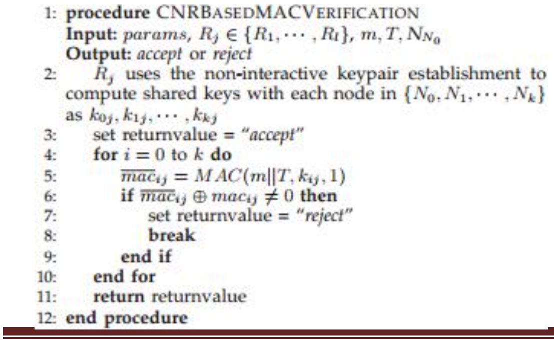
•) First, we study the random graph characteristics of wireless sensor node deployment, and estimate the probability of k-neighbors, which provides the necessary condition for BECAN authentication;

•) Second, we propose the BECAN scheme to filter the injected false data with cooperative bit-compressed authentication technique. With the proposed mechanism, injected false data can be early detected and filtered by the en-route sensor nodes. In addition, the accompanied authentication information is bandwidth-efficient; and

•) Third, we develop a custom simulator to demonstrate the effectiveness of the proposed BECAN scheme in terms of en-routing filtering probability and false negative rate on true reports.

1. **Early detecting the injected false data by the en-route sensor nodes**

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 many injected false data flood into the sink, the sink will surly suffer from the Denial of Service (DoS) attack.



```
procedure CNRBASEDMACVERIFICATION
    Input: $params,\ R_j \in \{R_1, \cdots, R_l\}, m, T, N_{N_0}$
    Output: $accept$ or $reject$
    $R_j$ uses the non-interactive keypair establishment to compute shared keys with each node in $\{N_0, N_1, \cdots, N_k\}$ as $k_{0j}, k_{1j}, \cdots, k_{kj}$
    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
```

2. **Gang Injecting False Data Attack**

We introduce 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.

2. **Reliability of the BECAN scheme**

In addition to the high (en-routing) filtering probability, the BECAN scheme also has high reliability, i.e., even though some sensor nodes are compromised, the true event reports still can reach the sink with high probability. Let FNR be the false negative rate on the true reports and tested as

$$\text{FNR} = \frac{\text{number of true data that cannot reach the } sink}{\text{total number of true data}}$$

If FNR is small, the BECAN scheme is demonstrated high reliability.

4. RESULT

We now analyze the security of our proposed scheme to authenticate the measurement reports. The performance metrics include (i) filtering efficiency is defined as the probability of false data to be filtered out within a number of hops, (ii) attack resilience is defined as the ratio of compromised components (clusters) vs. the total components (clusters) in the system, and (iii) filtering capability is defined as the average forwarded hops of false measurement reports, i.e., the average hops that the false measurement report will be forwarded before being detected and filtered. The overhead analysis of PCREF in terms of storage and energy cost can be found.

A.FILTERING EFFICIENCY

PCREF requires that each legitimate measurement report attaches T valid MAPs. When the attacker compromises x(x < T) sensing nodes in the cluster and obtains x authentication polynomials to derive x valid MAPs, he has to attach other forged T −x MAPs in the forged report in order to successfully send the forged measurement to the controller.

We have

$$Ph = (1 - pf)\ h{-}1 \cdot Pf;$$

$$P'h = 1 - (1 - Pf)\ h:$$

The filtering efficiency of PCREF can be represented by P'h defined as the probability of false measurement report to be filtered within a number of hops. Obviously, the greater the probability, the better the filtering efficiency becomes.

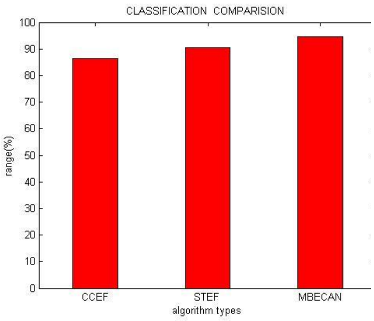
B. RESILIENCE TO ATTACK :The node impersonating attack against the legitimate node. According to the filtering rules of PCREF, the measurement report is false if more than one MAP carried in the report is not derived from the primitive polynomial assigned to the cluster, where the report generates.

1: Use the check polynomial and authentication polynomial stored in compromised sensing nodes and forwarding nodes to derive the primitive polynomial of the target cluster and derive enough valid authentication polynomials via the derived primitive polynomial.

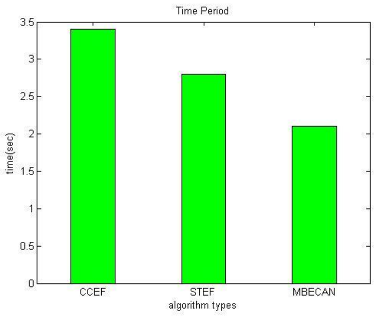
2: Compromise T or more sensing nodes in the target cluster and obtain authentication polynomials stored in them

This table shows the value of accuracy and time period for existing and proposed algorithm

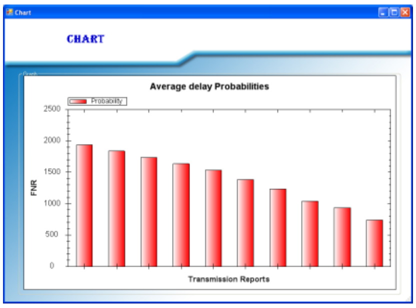
S.No	Algorithm	Accuracy	Time period
1	CCEF	86.4	3.3
2	STEF	90.5	2.5
3	MBECAN	96.8	1.5



Accuracy comparison methods



Time period comparison method



4. CONCLUSION

Proposed BECAN scheme for filtering the injected false data has been demonstrated to achieve not only high en-routing filtering probability but also high reliability with multi-reports. Due to this the BECAN scheme could be applied to other fast and distributed network were the authentication purpose is also distributed, e.g., authentication function in the wireless mesh network. BECAN does not require a complex security fixation because it uses a no interactive key establishment.

In addition, BECAN considers the situation that each node could be compromised; hence it distributes the en-routing authentication information to all sensor nodes on the routing path. It also adopts the bit-compressed authentication technique to save the bandwidth. Therefore, it is very suitable for filtering false data in wireless sensor networks and hence compromise-tolerant. In our future work, we will investigate how to prevent or reduce the gang injecting false data attack from mobile compromised sensor nodes. In this paper, we have proposed a novel BECAN scheme for filtering the injected false data. This scheme achieves not only high en-routing filtering probability but also high reliability with multi-reports and timestamp.

Due to this the BECAN scheme could be applied to the other fast and distributed network where authentication purpose is also distributed, e.g., authentication function in wireless mesh network. BECAN does not require complex security fixation because it uses non-interactive key establishment. In our future work, we will investigate how to prevent or reduce the gang injecting false data on mobile compromised sensor nodes.

REFERENCES

[1] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014.

[2] V.Chitra, L.Hameetha Begum, M.Ramya, R.Udhaya," Filtering False Data Injection Using Becan Scheme in Wireless Sensor Networks", IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014.

[3] Amuthan Mathy.P, Gowri Sankar.U, "Filtering Injected False Data in Wireless Sensor Networks by Using L, F, S Nodes and Key Distribution", International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014.

[4] Laxmi Shabadi, Snehal .T, Sanjana .H, Kalavati .G, Anita .K, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data using timer in Wireless Sensor Networks", International Journal of Emerging Engineering Research and Technology Volume 2, Issue 3, June 2014.

[5] Xinyu Yang, Jie Lin, Paul Moulema,Wei Yu, Xinwen Fu and Wei Zhao, "A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems", 2012 32nd IEEE International Conference on Distributed Computing Systems.

[6] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, and Xuemin (Sherman) hen, Fellow, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 1, JANUARY 2012.

[7] [7] X. Lin, R. Lu, and X. Shen, "MDPA: Multidimensional Privacy- Preserving Aggregation

Scheme for Wireless Sensor Networks," Wireless Comm. and Mobile Computing, 2010.

[8] [8] X. Lin, "CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks," IEEE GLOBECOM 2009.

[9] [9] V.C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in Wireless Sensor Networks," Wireless Comm. and Mobile Computing, Jan. 2008.

[10] [10] K. Ren, W. Lou, Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," IEEE Sensor Ad Hoc Comm. Networks (SECON '07), June 2007.

[11] [11] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," IEEE INFOCOM '06, Apr. 2006.

[12] [12] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks," IEEE J. Selected Areas in Comm. 2006.

[13] [13] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks," IEEE INFOCOM '04, Mar. 2004.

[14] [14] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by- Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," IEEE Symp. Security and Privacy, 2004 [8] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Ninth ACM Conf. Computer and Comm. Security, 2002

AUTHOR

1. Mr.A.P.Thangamuthu has completed his MCA and having teaching experience of 6 years. At present he is working in SNMV College of Arts and Science. His area of of specialization is Network Security.

2. Mrs.B.Chithra is persuing Ph.D in computer science. She is the Head of Computer Technology Department in SNMV College of Arts and Science. She is Having 10 Years of teaching experience. Her area of interest is Data mining.