IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON MISSION CRITICAL SENSORS AND SENSOR NETWORKS (MC-SSN)

Received November 1, 2018, accepted November 22, 2018, date of publication November 29, 2018,
date of current version December 27, 2018.

*Digital Object Identifier 10.1109/ACCESS.2018.2883474*

# Deterministic En-Route Filtering of False Reports: A Combinatorial Design Based Approach

**ALOK KUMAR AND ALWYN R. PAIS**

Information Security Research Lab, Department of Computer Science and Engineering, National Institute of Technology Karnataka–Surathkal, Mangalore 575025, India

Corresponding author: Alok Kumar (alok_21@outlook.com)

**ABSTRACT** Wireless sensor networks are an easy target for report fabrication attack, where compromised sensor nodes can be used by an adversary to flood the network with bogus/false reports. En-route filtering is a mechanism where intermediate forwarding nodes identify and drop false reports while they are being forwarded toward the sink. Most of the existing en-route filtering schemes are probabilistic, where sensor nodes in each cell share secret keys with a fixed probability with intermediate nodes. Thus, forwarded reports are verified probabilistically by intermediate nodes, because of which false reports can travel several hops before being dropped. Few deterministic en-route filtering schemes have also been proposed in the literature, but all such schemes require a source to send the reports through a fixed path to reach the sink. In this paper, we propose a novel deterministic en-route filtering scheme based on a combinatorial design to overcome the above-mentioned limitations of the existing schemes. The use of combinatorial design-based keys ensures direct communication between all the sensor nodes while maintaining low key storage overhead in the network. We provide a comprehensive analysis of the proposed scheme. The proposed scheme notably performs better than the existing schemes in terms of the expected filtering position of false reports. Furthermore, the proposed scheme improves data authenticity in the network and is more buoyant to selective forwarding and report disruption attacks.

**INDEX TERMS** Combinatorial design, false data detection, en-route filtering, wireless sensor networks (WSNs).

## I. INTRODUCTION

Broad applications of Wireless Sensor Networks (WSNs) have attracted a lot of attention from the researchers in recent times. WSN consists of a large number of sensor nodes which have limited memory space, restricted power resources, limited computation capacity, and short range radio communication capabilities. Typical WSN offer capabilities to monitor a physical environment which enables WSN to be implemented in applications such as vehicle safety monitoring, alarm systems, military surveillance, etc. [1].

Usually, WSNs are installed in inhospitable environments. Thus, WSNs are prone to several security threats such as sybil attack, wormholes, selective forwarding attack [2]. An adversary can perform node replication attack [3] or code injection attack [4] to compromise several sensor nodes in the network. Further, an adversary can obtain the cryptographic keys [5] from the compromised sensor nodes. Compromised sensor nodes can be used by the adversary to inject bogus/false data traffic in the network. This can cause sink to reckon a wrong system states [6], which can be troublesome for mission critical feedbacks. Further, such attacks abuse network resources like bandwidth, energy and can cause network congestion [7]. The solution to such attacks is collaborative endorsement and en-route verification of each report.

In the last two decades, several en-route filtering schemes have been proposed [8]–[16]. However, all these schemes have associated limitations. For example, GRSEF [13], PCREF [14] are prone to selective forwarding attack. SEF [8], IHA [15] are susceptible to T-threshold limitation [17]. STEF [11] and CCEF [12] require reports to be sent through a fixed path. LEDS [9] and LBRS [10] are prone to node failure and DoS attacks [18].

In this article we propose a novel deterministic combinatorial design based en-route filtering scheme. Different for existing deterministic schemes, the proposed design does not require sending reports through a fixed pre-defined path. Further, because of the deterministic nature of the proposed scheme, filtering efficiency of the proposed scheme

is excellent. For the proposed scheme we assume a distributed WSN, where the deployment network is partitioned into equi-sized cells. Further, we have two different types of sensor nodes in each cell namely, Cluster Heads (CHs) and ordinary sensor nodes. In the proposed scheme, we assign pair-wise keys to the sensor nodes to secure communication between them and cluster heads/sink. For en-route data endorsement/verification, we assign keys to the CHs based on combinatorial design. Thus, all the CHs can communicate with each other without alarmingly increasing key storage overhead in the network. In the proposed scheme reports are forwarded and verified only by CHs. This helps in reducing the energy requirements in sensor nodes while maintaining desired security in the network. This also helps in reducing the effect of selective forwarding attack in the network. In the proposed scheme similar to [19], each cell has three CHs and all the three CHs participate in report generation. So, three copies of each report with different endorsements are forwarded in the network, which considerably improves data authenticity in the proposed scheme. We further define a novel beam model for each cell which identifies all the upstream and downstream cells. Based on upstream and downstream cells, keys stored in each CH are further reduced. This helps in reducing the overall key storage overhead in the network.

Major contributions of the article are as follows:

- We have proposed a novel deterministic en-route filtering scheme based on a combinatorial design for WSNs.
- We have proposed a novel beam model to identify the upstream and downstream region of each cell to reduce key storage overhead.
- We have proposed a novel report endorsement and verification technique for more effective en-route filtering of false reports.

### A. RELATED WORK

#### 1) EN-ROUTE FILTERING SCHEMES

To detect and filter false data in WSNs, several en-route filtering schemes have been proposed [8]–[16]. All the existing en-route filtering schemes can be classified based on the sharing of keys [17] and can be grouped into 3 classifications namely probabilistic, deterministic and hybrid.

In probabilistic schemes, all the sensor nodes in the network exchange keys with randomly selected intermediate sensor nodes with a fixed probability. In SEF [8], sensor nodes are assigned a fixed number of secret keys chosen from a global key pool. Because of which multiple sensor nodes share few keys and using these keys intermediate sensor nodes can verify the authenticity of each forwarded report. In GRSEF [13], sensor nodes are assigned keys based on the division of deployment region along multiple axes. PCREF [14] adopted polynomials in place of secret keys for report's endorsement and verification. Akram and Cho [20] proposed a fuzzy logic based en-route filtering scheme. In the scheme [20], verification nodes for each cell are selected using fuzzy logic to improve the energy efficiency in the network. But SEF [8], GRSEF [13], PCREF [14] and scheme [20] are prone to report disruption and selective forwarding attacks.

In deterministic schemes, sensor nodes interchange secret keys with fixed intermediate sensor nodes on the path from source to the sink. Thus, all the intermediate sensor nodes have a probability of 1 to check the authenticity of each report. In IHA [15], each sensor node maintains a pair-wise key with a chosen intermediate sensor node on the path from source to the sink. Because of which IHA [15] is prone to T-threshold limitation [17]. STEF [11], CCEF [12] and PKCCEF [21] are ticket based schemes, where the sink produces a ticket for each CH and these tickets are then sent to the appropriate CH. After receiving the ticket, cluster head attaches the ticket with the final report. Then, the final report is forwarded through the same path to the sink. Thus all the deterministic schemes [11], [12], [15], [17] require reports to be sent through a fixed path. In PKCCEF [21], multiple paths are maintained between sensor nodes, but still, number of paths are limited and it further results in added key storage overhead.

Hybrid schemes, on the other hand, uses both deterministic and probabilistic approaches to assign keys to the sensor nodes. Applying deterministic approaches, LBRS [10] creates an arc of upstream cells whose reports a particular cell will forward, whereas in LEDS [9] each cell identifies only a few neighboring upstream cells. In probabilistic methods, sensor nodes in each cell select few intermediate sensor nodes probabilistically from upstream cells and exchange secret keys with them. These hybrid methods [9], [10] promises average filtering efficiency with limited key storage overhead.

#### 2) COMBINATORIAL DESIGN BASED KEY PRE-DISTRIBUTION SCHEMES

Çamtepe and Yener [22] were the first to use the combinatorial design for key pre-distribution in WSNs. Further, they provided a mapping of combinatorial design based key sharing to the sensor networks. They adopted generalized quadrangles and projective planes for proposing key pre-distribution scheme. This presented a foundation stone for research in this area, which resulted in many new schemes based on different combinatorial designs being proposed for key pre-distribution in recent times.

Lee and Stinson [23] gave a formal definition of using combinatorial design to propose key pre-distribution. They proposed the concept of common intersection designs for key pre-distribution.

Chakrabarti *et al.* [24] merged multiple blocks in combinatorial design to present a hybrid key pre-distribution scheme. They adopted the same method of block generation using transversal design as discussed by Lee and Stinson [23] and they merged them to create new blocks.

Ruj and Roy [19] proposed a novel key pre-distribution scheme based on combinatorial design for a grid-group based WSNs. Key pre-distribution and shared key discovery in

the proposed scheme is based on transversal design, much similar to as discussed in [23]. For the scheme, the authors adopted a heterogeneous network which has two types of sensor nodes namely, ordinary sensor nodes and agents. Intra-cell communication in the network is direct and for inter-cell communication, agents are used. In the proposed scheme, the number of agents in each cell is fixed to three.

Kumar and Pais [25] proposed a hybrid key pre-distribution scheme for WSNs. In the scheme [25], combinatorial design based keys secure intra-cell communication and pair wise keys ensure inter-cell communication. This setup is perfect for one-to-one communication between sensor nodes in the network. But in the data collection and en-filtering scenarios in a WSN, we are looking at many-to-one data forwarding/verification. In such cases, the scheme [25] results in high key storage overhead and low resiliency against compromised nodes in the network.

Bag and Roy [26] adopted Blom's scheme [27] and proposed key pre-distribution scheme for WSNs. The proposed scheme is then mapped to a grid-group deployment of sensor nodes in a heterogeneous network (ordinary sensor nodes and agents) same as done by Ruj and Roy [19].

Kumar and Pais [28] proposed another scheme for a heterogeneous network. Different from existing schemes, the proposed scheme used difference method or difference method [29] to construct key blocks. Further, key assignment to cluster head was done in such a manner, which ensured better resiliency than existing schemes.

### B. ORGANIZATION

The remaining article is organized as follows: Section II provides the needed basic concepts for the proposed scheme followed by an associated system and threat model. The proposed scheme is presented in Section III. Security analysis of the proposed scheme is provided in Section IV, followed by performance evaluation in Section V. Finally, we conclude our article in Section VI.

## II. PRELIMINARIES

### A. COMBINATORIAL DESIGN

A set system or a design [29] is a pair $(\mathcal{X}, \mathcal{A})$, where $\mathcal{X}$ is a set of elements (*varieties*) and $\mathcal{A}$ is a set of subsets of $\mathcal{X}$, called blocks $[\mathcal{A} = \{x : x \subseteq \mathcal{X}\}]$. A Balanced Incomplete Block Design (BIBD) [29] $(v, b, r, k, \lambda)$, is a design which satisfies the following conditions:

- $|\mathcal{X}| = v$, $|\mathcal{A}| = b$,
- The number of elements in each subset $\mathcal{A}$ is exactly $k$,
- Each *variety* in $\mathcal{X}$ occurs in $r$ blocks,
- Each pair of *varieties* in $\mathcal{X}$ is present in exactly $\lambda$ blocks in $\mathcal{A}$.

When $v = b$, BIBD is called a symmetric BIBD or symmetric design and is denoted by SBIBD $(v, k, \lambda)$ [29, Defination 2.1.1].

A *difference set* [29] $(v, k, \lambda)(mod\ v)$ is a set $\mathcal{D} = \{d_1, d_2, ..., d_k\}$, where $d_k$ represents a distinct element of $Z_v$, such that each element $d$, where $d \neq 0$ can be expressed in the form $d = d_i - d_j\ (mod\ v)$ in exactly $\lambda$ ways. Then blocks for symmetric design $(v, k, \lambda)$ can be easily obtained by $\mathcal{D}$, $\mathcal{D}$+1, $\mathcal{D}$+2, $\cdots$, $\mathcal{D}$+$(v-1)(mod\ v)$. For example, to generate (7, 3, 1) Symmetric design, difference set {1,2,4} can be used. All the resulting blocks will be : {1,2,4}, {2,3,5}, {3,4,6}, {4,5,7}, {5,6,1}, {6,7,2}, {7,1,3}.

A *multiplier* $(q)$ [30] of a given *difference set* $(\mathcal{D})$ for $(v, k, \lambda)$ in an *Abelian group* $(\mathcal{G}, +)$ satisfies following properties :

- $q$ is a prime number such that $gcd(q, v) = 1$ ,
- $q > \lambda$ such that $k - \lambda = 0(mod\ q)$.

### B. NOTATIONS

For convenience we discuss all the notations used in this article.

- $N$ : Total number of sensor nodes in the network
- $C$ : Total number of cells in the network
- $n$ : Number of sensor nodes in a particular cell
- $C_c$ : $(c)$th cell
- $CH_c^i$ : $(i)$th Cluster head in $(c)$th cell
- $(x_c, y_c)$ : Center location of a particular cell
- $x_{loc}$ : Geographical location of sensor node $x$
- $k + 1$ : Number of keys assigned to each sensor node
- $K_m, P^1, P^2, P^3$ : 4 master secret keys
- $K_x$ and $P_c^i$ : Secondary secret keys calculated by sensor node $x$ in cell $c$
- $M$ : Event report
- $M_x$ : Unique secret share for the report $M$ calculated by sensor node $x$
- $M_{encr}$ : Encrypted report
- $P$ : Large prime number
- $H$ : Hash function
- $T$ : Number of shares to be included with each report
- $t$ : Minimum number of correct shares required in each report to recover the event report $M$

### C. SYSTEM MODEL

- We assume a distributed sensor network with $N$ sensor nodes for the proposed scheme which is partitioned into equi-sized cells. Each cell has $n$ sensor nodes in the network. Further, there is a sink in the network which verifies/collect all the reports.
- Each cell has two types of sensor nodes namely, Cluster heads and ordinary sensor nodes.
- For the proposed scheme, we have three cluster heads in each cell similar to [19]. Further, we have three types of key sets namely, *Type* 1, *Type* 2 and *Type* 3 generated from different key pools. These key sets are assigned to all the cluster heads such that different types of key-sets are assigned to all three cluster heads in each cell. Thus, each CH can communicate with CHs of the same type in the whole network.
- Cluster heads can obtain their geographical location via any localization scheme [31], [32] or using in-built

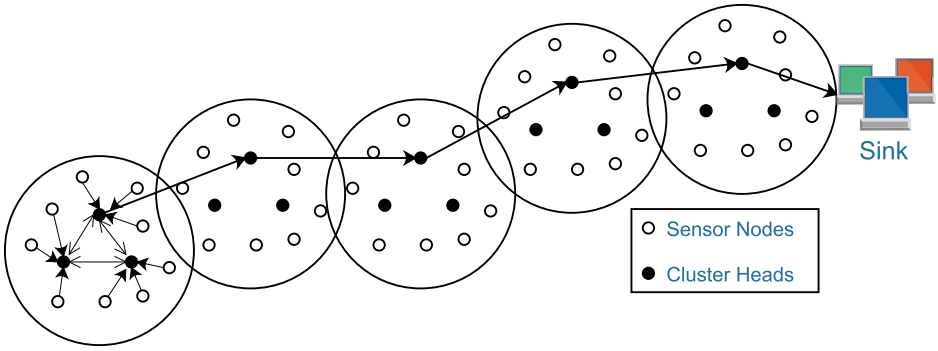


**FIGURE 1.** System model.

GPS [33]. The proposed scheme can tolerate location errors as only centers of the home cell are used for the scheme.
- Each event in the network is detected by multiple sensor nodes. All the sensor nodes which detect the event, generate the report and send it to the CHs. Cluster heads then forward the final report to the sink via multi-hop path.
- Reports verification and report forwarding are only done by CHs in the network.
- All the sensor nodes and CHs have unique IDs.

Figure 1 provides the system model for the proposed scheme.

### D. THREAT MODEL

We assume CHs and sensor nodes can be compromised by an adversary. When an adversary compromises a sensor node/CH, all the information stored in it is revealed to the adversary. Using the obtained information, an adversary can inject false packets and drop/alter genuine packets. However, an adversary cannot compromise the sink.

## III. PROPOSED SCHEME

Now, we explain the process of sensor nodes deployment, sensor node initialization, secret keys allotment, and shared key discovery phase. Further, we discuss report generation and en-route filtering in the WSN.

In the proposed scheme, we use pair-wise keys for data authentication between sensor nodes and cluster heads/sink. For data endorsement/verification of the forwarded reports, we assign combinatorial design based keys to cluster heads, which ensures low key storage overhead and very effective en-route filtering of false reports. This way of the key assignment is almost reverse to what was proposed in our other scheme [25], where we assigned combinatorial design based keys to sensor nodes to secure intra-cell communication in the network and pair-wise keys to few sensor nodes in each cell to secure inter-cell communication. This was mainly done keeping in mind one-to-one communication between sensor nodes in the network for the scheme [25]. On the other hand in our scenario, where we collect data from the sensor nodes at a sink, we have many-to-one communication in the network. Thus, we adopted pair-wise keys for intra-cell data collection/authentication and combinatorial design based keys for inter-cell data authentication.

For the proposed scheme, we modify existing symmetric design from [28] to assign keys to cluster heads in the network. For the same, we propose a novel beam model for further reduction in keys stored by each cluster heads without affecting the filtering efficiency of the network. Finally, we propose a novel report generation, novel en-route filtering/sink verification methods which ensure improved data authenticity and data availability in the proposed scheme.

### A. DEPLOYMENT

For the key assignment in sensor nodes and CHs, network administrator prepares 4 master secret keys ($K_m$, $P^1$, $P^2$, $P^3$). Administrator further chooses a large prime number ($P$), hash function $H(.)$, and the parameters $T, t$. The parameters $T, t$ were defined in [34], where $T$ represents the number of secret shares to be included in each report and $t$ represents the minimum number of correct secret shares required in each report to validate it.

### B. INITIALIZATION OF SENSOR NODES

Each sensor node in a particular cell is assigned $K_m$, $P^1$, $P^2$, $P^3$, $P$, $H(.)$, $(x_c, y_c)$, and $x_{loc}$, where $(x_c, y_c)$ is the center location of a particular cell $(C_c)$ and $x_{loc}$ is location of each sensor node $x$. Each sensor node $x$ computes the secret key $K_x$ using $K_m$ and $x_{loc}$ as $K_x = H(K_m|x_{loc})$, where $|$ represents concatenation operation. This key is used by $x$ to communicate securely with the sink. To secure communication with CHs in cell $C_c$, each sensor node $x$ uses other 3 master secret keys to generate secret keys $(P_c^1, P_c^2, P_c^3)$ as $P_c^i = H(P^i|(x_c, y_c))$. So, $P_c^1$ can be used by sensor node $x$ to securely communicate with $CH_c^1$. After computation of keys in a sensor node, all the master secret keys are removed by it. The secret key generation process is done by each sensor node in the network.

### C. INITIALIZATION OF CLUSTER HEADS

Each CH is assigned one master key $P^i$, such that $P^1, P^2, P^3$ are individually assigned to three CHs in a particular cell.

Cluster heads can use this master key to securely communicate with sensor nodes in the cell. In addition to the master key, CHs are also assigned $T$ and $(x_c, y_c)$. For enabling en-route filtering in the network, CHs are assigned keys based on combinatorial design. In the proposed scheme, each type of CHs are assigned keys from different key pools, limiting communication of CHs among the same type. If total number of cells in the network are $C$, then there are $C$ CHs for each type *Type* 1, *Type* 2 *and Type* 3. Cluster heads of a particular type are assigned keys based on symmetric design as explained in Section II.

For the symmetric design, we adapt [28]. According to the adopted scheme, initially, the value of $k$ is decided such that $C <= k^2 + k + 1$, where $k$ is the smallest prime number. Variable $k$ can now be used to define the desired symmetric design $(k^2 + k + 1, k + 1, 1)$. In the proposed scheme we used *difference set* [29] for construction of symmetric design. Equivalent difference set for the desired symmetric design is $(k^2+k+1, k+1, 1) mod (k^2+k+1)$. Steps for such a design construction are given below:

- Initially, multiplier of the difference set $(k^2 + k + 1, k + 1, 1)$ in an *Abelian group* $(Z_{k^2+k+1}, +)$ is defined.
- Derive all the orbits of the given *Abelian group* $(Z_{k^2+k+1}, +)$ using the multiplier defined in the previous step.
- Any subsets of the orbits can be combined to derive the difference set $(D)$ of set size $k + 1$.
- All the blocks are derived using the obtained difference set $D$ for the equivalent symmetric design $(k^2 + k + 1, k + 1, 1)$.

**Algorithm 1** Blocks Generation Using Symmetric Design

**INPUT** - Symmetric design $(v, k, \lambda)$ where $\lambda = 1$
**OUTPUT** - $k^2 + k + 1$ blocks of keys, each block has $k + 1$ keys and any two blocks have one shared key
**STEPS**- 1. Find Multiplier $(a)$ for difference set $(D)$.
2. Compute all the orbits by mapping $x \longmapsto ax \ mod \ v$.
3. Find *difference set* $\{d_1, d_2, ..., d_{k+1}\}$ of $(k+1)$ length using the orbits.

```
For j ← 1 to (k^2 + k + 1) do
        Block_j= {d_1, d_2, ..., d_{k+1}}
        For i ← 1 to (k + 1) do
                {d_i = (d_i + 1) mod (k^2 + k + 1)}
        end for
end for
```

Further details regarding blocks generation using difference set can be obtained from [29] and [30]. These key blocks are then randomly assigned to all the CHs of the same type. Construction algorithm for the same is given in Algorithm 1 which takes $O(k^3) = O(C^{1.5})$ time. Symmetric design in key blocks generation ensures that any pair of key block shares few keys. So assignment of a key block to a CH ensures that it can verify all the reports from other CHs of the same type, that too without any shared key discovery. Moreover, adoption of symmetric design for key block generation helps in providing a deterministic way of sharing secret keys in the network while maintaining marginal key storage overhead. At the time of report generation, CH creates and append $k + 1$ MACs using its key block to the final report. When this report is forwarded through the network, each intermediate CH of the same type checks the authenticity of the report by verifying the MACs attached with the report.

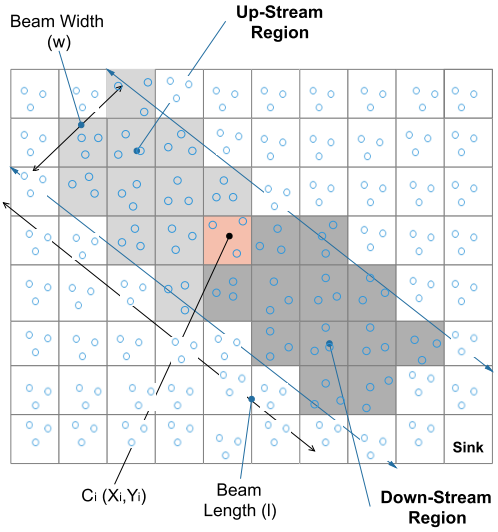


**FIGURE 2.** Beam model implementation in the network.

#### 1) MODIFICATION OF KUMAR AND PAIS'S SCHEME

When the reports are forwarded from an event cell toward the sink, they follow a narrow beam like path to reach the sink i.e. each report is forwarded only through a limited part of the network. Thus, we do not need all $k + 1$ MACs with each report. In the proposed scheme to reduce the number of MACs required with each report and to reduce the keys stored in each CH, $Cell - Upstream$ region and $Cell - Downstream$ region for each cell is defined. Figure 2 shows $Cell - Upstream$ region and $Cell - Downstream$ region for a cell $C_i$. In a normal network, CHs of cell $C_i$ have to verify reports only from its Upstream region and any report being sent by cell $C_i$ is only verified by Downstream region. Thus, CHs in cell $C_i$ need keys shared only within $Cell - Upstream$ and $Cell - Downstream$ region. For shared key discovery in $Cell - Upstream$ and $Cell - Downstream$ region, we create *report verification* and *report endorsement* key list. Both key list construction is discussed in the next subsection.

### D. CREATION OF REPORT VERIFICATION AND REPORT ENDORSEMENT KEY LIST

$Cell - Upstream$ region and $Cell - Downstream$ region for a particular cell are determined by the cell's and sink's location in the network. Both regions are represented by a parallel beam in the direction of the cell from the sink. Further, the beam width $(w)$ and beam length $(l)$ are variables (Figure 2) and can be chosen by network administrator accordingly. Specifically, *Upstream* and *Downstream* regions

for a particular cell represents a rectangular area around it and all the cells which are covered in this area are identified by the cell using simple geometry. All these calculations can be done by any CH of each cell to identify other cells in both the upstream and downstream region. This information is then forwarded to other CHs in the same cell. Upstream region for a particular $CH_c^i$ covers all CHs whose report it can forward and verify. Further, the downstream region for a $CH_c^i$ covers all CHs who can verify the reports sent by it. Thus, $CH_c^i$ creates two keys lists namely, *report verification* key list and *report endorsement* key list. Both the key lists are created by each CH by identifying common secret keys shared with other CHs in upstream and downstream region respectively.

For the creation of key lists, each $CH_c^i$ creates a message containing key indexes of all the keys stored in it. This message is then broadcasted in the network. When a particular $CH_j^i$ receives this broadcasted message, $CH_j^i$ checks whether $CH_c^i$ is in its upstream region or downstream region. If true and $CH_c^i$ and $CH_j^i$ are of the same type, $CH_j^i$ identifies the shared key using key indexes from the message and it appends this secret key in either report verification key list or report endorsement key list accordingly. This process of broadcasting the message is recapitulated by all the CHs in the network. So, the communication overhead for both key lists generation is $O(m)$, where $m$ is the length of key indexes for all the keys stored in any CH. The identification of shared key takes only $O(1)$ time. After the process of shared key discovery and key list generation, initial key block assigned to each CH can be deleted by all the CHs, as now only *Report verification* key list and *Report endorsement* key list are used by CHs for report endorsement and report verification.

This process of creating two different key lists in each CH helps to reduce the keys stored in each CH and also helps to reduce the number of MACs to be sent with each report. Further details are discussed in Section V-B.

### E. REPORT GENERATION

When an event happens, any $2T$ sensor nodes in a particular cell agrees on the event report using technique given in [35]. A typical report $M$ contains information about the type of event, location, time of an event, etc.. After the agreement between sensor nodes for the report, each participating sensor node $x$ creates a unique share $M_x$ for the report with the predefined threshold $(t, T)$ *LSSS* [9]. Precisely, $M_x$ is derived by evaluating the polynomial (Equation 1) over $GF(P)$, where $GF(.)$ is a finite *Galois field* [36], $P$ and $t$ are pre-assigned parameters, $K_x$ represents secret exchanged between $x$ and sink, full partition of $M$ is denoted by $p_i$ where $i$ belongs to 0 to $t-1$.

$$M_x = \sum_{0 \leqslant i < t} p_i K_x mod(P) \tag{1}$$

This polynomial evaluation is done by all the participating sensor nodes using their own secret key shared with the sink. As $M_x$ is uniquely generated by each sensor node, it can be used by the sink as an endorsement. Further, node $x$ encrypts the original report $M$ using other three secret keys $P_x^1$, $P_x^2$, $P_x^3$ as $M^i encr = E_{P_x^i}(M)$. Finally, sensor node $s$ sends the tuple $\{M_x, x_{id}, M_{encr}^i\}$ to each CH in the home cell by attaching appropriate $M_{encr}^i$.

All the three CHs in the event cell collects all the $2T$ tuples from the participating sensor nodes. Initially, the freshness of all the secret shares included in the tuples is verified. Cluster heads also check whether the participating sensor nodes are from the home cell or not. Now, all three CHs coordinate with each other to choose $T$ tuples from $2T$ tuples such that each CH chooses at-least 50% different tuples when compared with the other two CHs. Selection of different tuples by each CH helps to improve the data authenticity of the proposed scheme and because of which the proposed scheme is more resilient to report disruption attacks. Further details for the same is given in Section IV. After choosing $T$ tuples, each CH decrypts $M_{encr}^i$ from each tuple to check whether $M$ sent by all nodes is the same or not. Further, CHs co-ordinate to find whether at-least two CHs have got all correct $M$. Next, each CH create MACs for the report $M$ using all the keys from the report endorsement key list. Finally, each CH prepares the final report of the form $\{M_1, M_2.., ID_1, ID_2.., M, MAC_1, MAC_2..MAC_{k_i}, ID_{k_1}, ID_{k_2}..ID_{k_i}\}$, where $MAC_{k_i}$ are the MACs generated using $k_i$ keys from the endorsement list and $ID_{k_i}$ are the key indexes. The final report is then forwarded by each CH towards the sink through the same type of CHs. In the proposed scheme each cell has three CHs, thus each event results in three different copies of the same report. But in Section V we will observe that even 3 copies of the same report do not increase the overall energy requirements for the proposed scheme.

### F. EN-ROUTE FILTERING AND SINK VERIFICATION

When any intermediate CH receives a report, it checks for the common key used for creating any MAC in the report. If no such key is found by the CH in its *report verification* key list, the report is dropped immediately. Else, the CH generates the MAC using the common secret key and compares it with the MAC included in the report. If both the MACs matches, the report is assumed to be correct, else it is dropped. Further, all three CHs in the forwarding cell co-ordinate with each other to identify whether at-least two copies of the report are found to be correct or not, if yes, then only correct copies of the report are forwarded to next hop, if not, all the copies of the report are dropped immediately.

Sink, on the other hand, performs *2-way authentication* for verifying each report. Sink starts the verification process of the report if it receives at-least two copies of the same report from two different types of CHs. Initially, sink verifies the freshness of all the $M_x$ included in the report and checks whether all the participating sensor nodes are from the same cell or not. Next, sink verifies all the MACs included with the report. If all the MACs are found to be correct, sink tries to recover $M$ from $M_x$. This can be done by recovering $M$ from any $t$ correct $M_x$ included in the report. More specifically,

sink picks any $t$ shares out of $T$ shares and tries to solves a $t$-variable linear equation (Equation 1) to get $p_i$, where $i = [0, t-1]$ and thus obtains $M$. If $M$ is meaningful, the recovery is successful, otherwise sink tries other combinations of $t$ shares to recover $M$. In the proposed scheme, sink receives at-least two copies of each report, where each copy contains at-least 50% different $M_x$ from other. Thus, in the worst case where sink only receives two copies of a report, until no more than $((3/2)T-t)$ invalid $M_x$ are present, the sink can always recover the original report.

## IV. SECURITY ANALYSIS OF THE PROPOSED SCHEME

In this section, we illustrate the security strengths of the proposed scheme in terms of data authenticity, expected filtering of false reports and data availability. But prior to that, we describe the simulation settings.

**TABLE 1. Simulation parameters.**

| Parameters | Values |
|---|---|
| Number of Sensor nodes | 10005 |
| Total number of Cells | 667 |
| Total sensor nodes in each cell | 15 |
| Cell Size | $50X50m^2$ |
| Cluster Heads in each cell | 3 |
| Communication range of Sensor nodes | $25m$ |
| Communication range of Cluster Heads | $50m$ |
| Beam Width ($w$) | $250m$ |
| Beam Length ($l$) | $500m$ |
| $(T, t)$ | 5,4 |
| Size of Report | 36 Bytes |
| Size of MAC | 4 Bytes |
| Energy Consumed to generate MAC | $15\mu J$(Per Byte) |
| Energy Consumed to verify MAC | $75\mu J$ |
| Energy Consumed to Transmit/Receive | $16.25/12.5\mu J$(Per Byte) |

The proposed scheme is evaluated in a custom built python simulator. The simulation parameters for the proposed scheme are given in Table 1. Further, there is a sink positioned in the center of the network. Typical parameter values for PCREF, LEDS and SEF are also same as discussed in Table 1. Further for PCREF and SEF, polynomial sharing probability or keys sharing probability $q$ is set to 0.2. For the simulations, compromised sensor nodes and cluster heads are chosen randomly in the network.

### A. DATA AUTHENTICITY

In the proposed scheme, at the time of report generation, each CH chooses $T$ tuples from $2T$ tuples in such a way that each CH has 50% different tuples. Further, at-least two CHs should agree with the tuple values and only then a report is generated and forwarded from the event cell. So an adversary can inject a bogus/false report which can successfully by-pass en-route filtering and sink verification only if:

1) Adversary is able to compromise at-least $(3/2)T$ sensor nodes in a particular cell. If total sensor nodes compromised in the network are $X$, then the probability that an adversary can successfully inject bogus report is given by

$$P_{Auth}(X) = \sum_{z=(3/2)T}^{n} \frac{\binom{n}{z}\binom{N-n}{X-z}}{\binom{N}{X}} \tag{2}$$

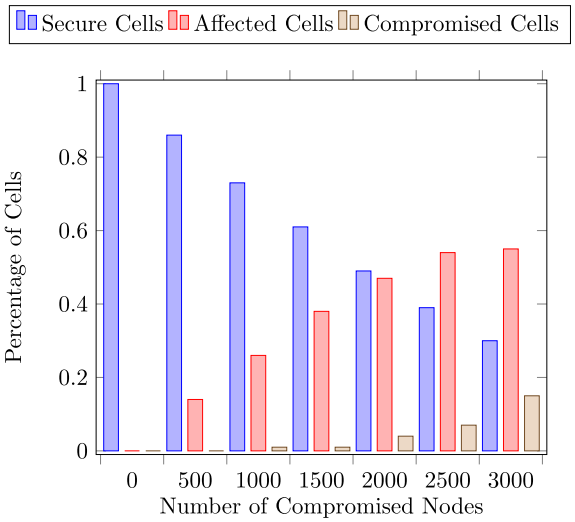


**FIGURE 3. Resiliency vs Compromised Nodes in the Proposed Scheme.**

2) Adversary is able to compromise at-least one CH and $T$ sensor node in a particular cell. If total sensor nodes compromised in the network are $X$, out of which $x$ are CHs, then the probability that an adversary can successfully inject bogus report is given by

$$P_{Auth}(X) = \sum_{z=T}^{n} \frac{\binom{n}{z}\binom{N-n}{(X-x)-z}}{\binom{N}{X-x}} \left( \sum_{i=1}^{3} \frac{\binom{3}{i}\binom{3C-3}{x-i}}{\binom{3C}{x}} \right) \tag{3}$$

3) Adversary is able to compromise at-least two CHs and $T$ sensor nodes in a particular cell. If given the number of sensor nodes compromised in the network are $X$, out of which $x$ are CHs, then the probability that an adversary can successfully inject bogus report is given by

$$P_{Auth}(X) = \sum_{z=T}^{n} \frac{\binom{n}{z}\binom{N-n}{(X-x)-z}}{\binom{N}{X-x}} \left( \sum_{i=2}^{3} \frac{\binom{3}{i}\binom{3C-3}{x-i}}{\binom{3C}{x}} \right) \tag{4}$$

The cases discussed above are the worst case scenarios where an adversary is able to inject bogus report from a particular cell, but in such scenario also remaining network is still un-compromised. The proposed scheme is better than schemes like LEDS [9] and PCREF [14] where adversary only requires $t$ and $T$ compromised sensor nodes in any particular cell respectively to inject bogus reports. Further, the proposed scheme is major improvement over schemes such as IHA [15], SEF [8], and LBRS [10], in which single compromised sensor node can result in multiple gains. Figure 3 provides the ratio of compromised cell vs total compromised sensor nodes in the network. In the figure we can observe that even when large number of sensor nodes/cluster heads are compromised, only few cells are totally compromised in the network. Figure 4 presents comparison among proposed scheme, SEF [8], LEDS [9] and PCREF [14] for data authenticity. The proposed scheme significantly outperforms SEF [8], LEDS [9] and PCREF [14] considerably.

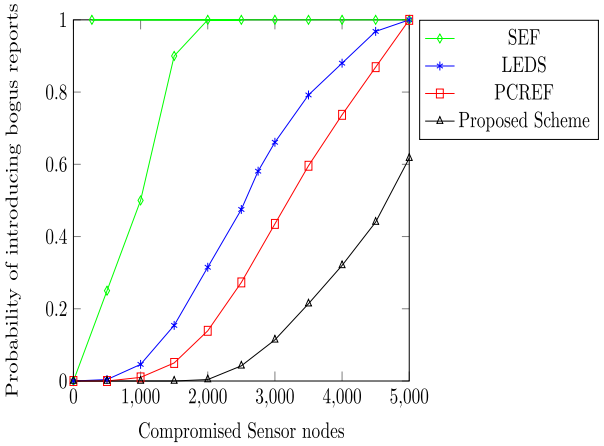


**FIGURE 4.** Data Authenticity in SEF [8], LEDS [9], PCREF [14] and the proposed scheme.

### B. EXPECTED FILTERING OF BOGUS REPORTS

The proposed scheme provides a deterministic en-route filtering mechanism where reports are verified by all the intermediate hops. In the proposed scheme we assign combinatorial design based keys to CHs. So if a CH is compromised, all its secret keys are exposed, affecting the other remaining network too. In the network because of the compromised CHs, at any point of time, a particular $CH_c^i$ can have its $y$ keys exposed out of total $Y$ keys. So, if an adversary wants to create a false report on behalf of $CH_c^i$, it has to forge other $(Y-y)$ MACs for successful report generation. To ensure this false report is dropped before it reaches the sink, one intermediate non-compromised CH is enough which has a key which was used to create any one of the $(Y-y)$ forged MACs.

In the network if $x$ sensor nodes are compromised and out of which $X$ CHs are compromised, then the probability of filtering a false report generated from $CH_c^i$ can be given by

$$P(X) = \sum_{x=0}^{H} (1 - P_{CH}^{x}) \frac{(Y-y)}{Y} \tag{5}$$

where $P_{CH}^{x}$ is the probability of any particular $CH_x^i$ being compromised and $H$ represents total hops between $CH_c^i$ and the sink. Further, $P_{CH}^{x}$ can be given as

$$P_{CH}^{x} = \frac{\binom{C}{X/3}\binom{3C-C}{X-(X/3)}}{\binom{3C}{X}} \tag{6}$$

where $C$ is total CHs of a particular type and $X/3$ represents compromised CHs of a particular type. But in the proposed scheme, 3 copies of each report with different MACs are forwarded toward the sink. So, to completely drop a false report from the network, at-least two copies of the same report must be dropped. Thus, the probability for completely dropping a false report from the network is given by

$$P_{filtering} = \binom{3}{2} P(X)^2 \tag{7}$$

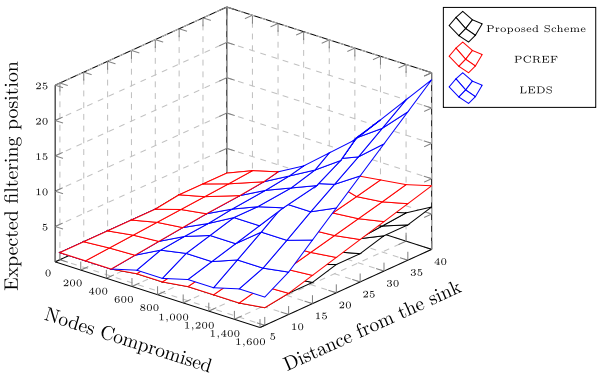


**FIGURE 5.** Expected filtering position of false reports in PCREF [14], LEDS [9] and the proposed scheme.

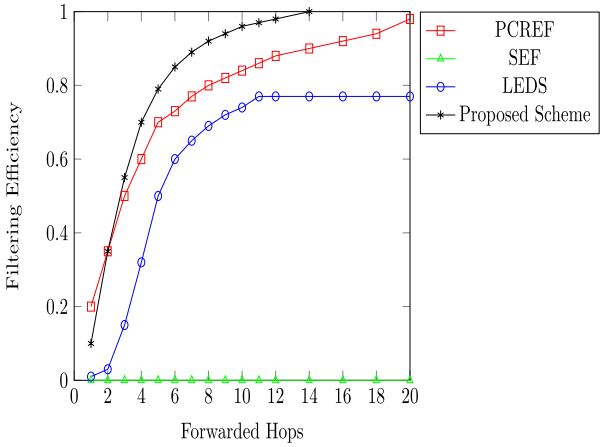


**FIGURE 6.** Filtering Efficiency vs Forwarded Hops in PCREF [14], LEDS [9], SEF [8] and the proposed scheme.

Experimental results of expected filtering position of the false report in the proposed scheme, LEDS [9] and PCREF [14] are given in Figure 5. In the figure we can observe that the proposed scheme filters the false reports in much less hops when compared with LEDS [9] and PCREF [14]. The main contributor for enhanced filtering efficiency is deterministic key pre-distribution in the CHs. Moreover, in the figure we can observe that the proposed scheme can filter false reports in 6 hops on average, which is a big improvement from 24 in LEDS [9] and 9 in PCREF [14]. Figure 6 provides the comparison of filtering efficiency vs hops traveled in PCREF, LEDS, SEF and the proposed scheme. From the figure, it is evident that the proposed scheme promises high filtering efficiency in the least number of hops. The filtering efficiencies of scheme such as IHA [15], LBRS [10] are always poorer than PCREF [14] as explained in [14], thus proposed scheme also has better filtering efficiencies than IHA [15], LBRS [10].

### C. DATA AVAILABILITY

Data availability in WSNs can severely be affected by two type of attacks namely, *Report Disruption* attack and *Selective Forwarding* attack. In Report Disruption attack,

compromised sensor nodes can intentionally send wrong tuples to CHs or compromised CHs can attach wrong MACs to the final report. Thus, correct reports are either dropped by intermediate CHs or by the sink because of wrong data in the report. On the contrary, compromised intermediate CHs can drop all the reports passing through them, this is termed as Selective Forwarding attack. Effect of both attacks on the proposed scheme is discussed in the next subsections.

#### 1) REPORT DISRUPTION ATTACK

In the proposed scheme, participating sensor nodes create the shares for the report and CHs generate MACs for the report. Thus, both compromised sensor nodes and compromised CHs can participate in report disruption attack. Compromised participating sensor nodes can send wrong $M_x$ with the tuple to the CH, so that sink cannot recover the original report. Further, Compromised CHs can attach wrong MACs with the reports, thus such reports are either dropped by intermediate CHs or sink. In the proposed scheme, each participating sensor node only contributes one share of the report follows (t,T) threshold LSSS [9], thus sink can always recover the correct report if it gets at-least $t$ correct tuples. Thus, correct reports are received and recovered by sink until:

- No CH is compromised and less then $2T - t$ participating sensor nodes are compromised in any cell. In the proposed scheme, $2T$ sensor nodes participate in report generation and if no CHs are compromised in the event cell, the sink will receive $2T$ tuples. Thus, the sink can use any $t$ correct tuples from $2T$ tuples to recover the correct report. Given the number of sensor nodes compromised in the network is $X$, the security strength of the proposed scheme in such a case can be given as:

$$P_{Avail}(X) = \sum_{z=0}^{2T-t} \frac{\binom{2T}{z}\binom{N-2T}{X-z}}{\binom{N}{X}} \tag{8}$$

- One CH is compromised and less than $(3/2)T - t$ sensor nodes are compromised in any cell. In the case where one CH is compromised, the sink will receive only two copies of the report because the third copy of the report will be dropped either by intermediate CHs or by sink due to in-correct MACs. Thus, the sink will only receive two copies of the report with total $(3/2)T$ tuples and sink can use any $t$ correct tuples from them to recover the correct report. Given the number of sensor nodes compromised in the network are $X$ out of which $x$ CHs are compromised, security strength of the proposed scheme in such case can be given as:

$$P_{Auth}(X) = \frac{\binom{3}{1}\binom{3C-3}{x-1}}{\binom{3C}{x}} \left( \sum_{z=0}^{(3/2)T-t} \frac{\binom{(3/2)T}{z}\binom{N-(3/2)T}{(X-x)-z}}{\binom{N}{X-x}} \right) \tag{9}$$

From the above discussed cases, we can conclude that the proposed scheme is more resilient than LEDS, where sink can recover the correct report only if compromised participating sensor nodes are less then $T - t$. Further, the proposed scheme is better than PCREF [14], SEF [8], IHA [15] and LBRS [10] where sink can recover the correct report only if all the MACs are correct.

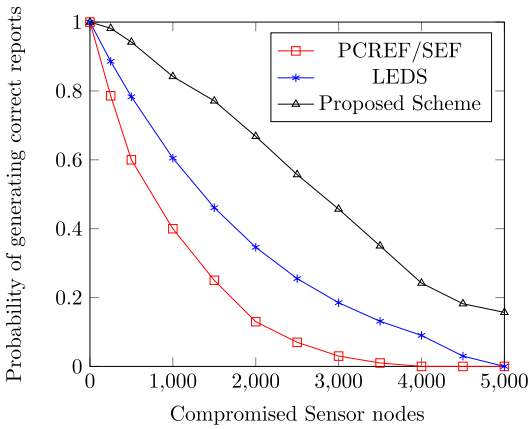


**FIGURE 7. Data Availability under Report Disruption attack in PCREF [14], LEDS [9], SEF [8] and the proposed scheme.**

Figure 7 provides the comparative experimental analysis of the proposed scheme with SEF [8], LEDS [9] and PCREF [14]. In the Figure 7, we can observe that SEF [8] and PCREF [14] performs equally against report disruption attack and LEDS [9] performs better then these schemes. Further, in the figure we can observe that the proposed scheme has more probability for generating correct reports than SEF [8], LEDS [9] and PCREF [14].

#### 2) SELECTIVE FORWARDING ATTACK

In the proposed scheme, three copies of same report are forwarded with different MACs from the event cell. Further, sink can accept the reports from the event cell if it receives at-least two copies of the same report through different type of CHs. So, in order to purposely drop a report and limit sink from obtaining the report, at-least two copies of the same report should be dropped before they reaches sink. To drop two copies of the same report, at-least two CHs of different types must be compromised on the path from event cell to the sink. Precisely, if a report originating from the event cell has to travel $H$ hops to reach the sink and in the network $x$ sensor nodes are compromised and out of which $X$ are CHs, then the probability that at-least one intermediate CH of a particular type is compromised can be given by

$$P_{com}(X) = \sum_{z=1}^{H} \frac{\binom{H}{z}\binom{C-H}{(X/3)-z}}{\binom{C}{X/3}} \tag{10}$$

Further, the dropping probability of a correct report in the proposed scheme can be given by

$$P_{select}(X) = \left\{ \binom{3}{2} (P_{com}(X))^2 (1 - P_{com}(X)) \right\} + (P_{com}(X))^3 \tag{11}$$

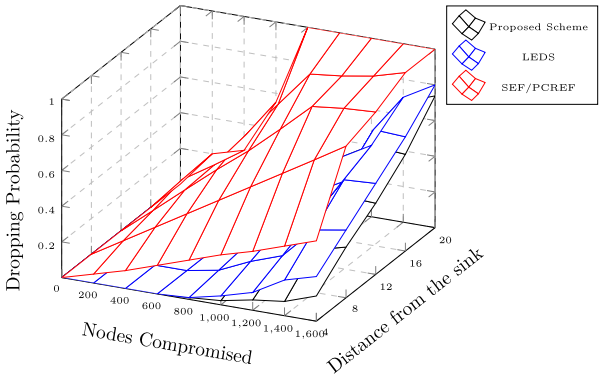


**FIGURE 8.** Data Availability under selective forwarding attack in PCREF [14], LEDS [9], SEF [8] and the proposed scheme.

Figure 8 presents the experimental comparison of the proposed scheme, SEF [8], PCREF [14] and LEDS [9]. In LEDS [9] at the time of report forwarding, each report is broadcasted to all the sensor nodes in an intermediate cell and because of which LEDS [9] is highly resilient to selective forwarding attack. But other existing schemes such as SEF [8], PCREF [14], LBRS [10], IHA [15] do-not adopt any preventive measures for selective forwarding attack because of which these schemes are highly prone to selective forwarding attack. We can observe from the Figure 8 that the proposed scheme outperforms LEDS [9] even without broadcasting reports in intermediate cells. This is mainly because in the proposed scheme sensor nodes do not participate in report forwarding. Thus, compromised sensor nodes cannot perform selective forwarding attack. Further from the figure, it is evident that the proposed scheme also significantly outperforms schemes such as SEF [8], PCREF [14].

## V. PERFORMANCE EVALUATION OF THE PROPOSED SCHEME

Now, we discuss the associated storage overhead, computation and communication overhead, and energy requirements for the proposed scheme.

### A. KEY STORAGE OVERHEAD

Each sensor node in the proposed scheme stores 4 secret keys, three for communicating with CHs in the same cell and one for communicating with the sink. On the other hand, CHs are assigned keys based on a combinatorial design where each CH is assigned $k + 1$ keys. Then, we deploy a beam model (Section III-D) to further decrease the number of keys stored in CHs by limiting secret keys shared only within the upstream and downstream region of a particular CH. If $C = 121$, then an average of 9 keys are stored in each CH. In LEDS [9], each sensor node is assigned $\{(T + 1)(T + 2)/2\} + 5$ keys. In PCREF [14], each sensor node is assigned large number of polynomials and secret keys which can be given by $(64.n_k + 16.n_c)$, where $n_k$ is total keys and $n_c$ is the number of coefficients. Thus, the proposed scheme has minimal storage overhead both in sensor nodes and CHs when compared with LEDS [9] and PCREF [14]. This is mainly due to use of symmetric keys which helps in maintaining full connectivity in the network without alarmingly increasing key storage overhead.

### B. COMMUNICATION AND COMPUTATION OVERHEAD

Computation and communication overheads in any scheme mainly arise because of initial key exchange, included MACs with the reports, and MAC verification. In the proposed scheme, we deploy combinatorial design based secret keys, which makes sure that any two CHs always share a secret key. Further, for shared key discovery, only a single message is sent by each CH in the network which is much efficient than 3-way handshake used in existing schemes like LBRS [10], LEDS [9], IHA [15]. For en-route filtering in the proposed scheme, each report is attached with multiple MACs. Each CH has to create MACs with the keys present in its *Report Endorsement* key list. For example, if total cells in the network are 121, then on an average each CH has 7 keys in *Report Endorsement* key list, thus on average 7 MACs are attached with each report. In such case communication overhead for the proposed scheme is 28 bytes, if the size of MAC is 4 bytes. In LEDS [9], $T + 1$ MACs are included with each report and thus total communication overhead is 24 bytes when $T = 5$. In PCREF [14] for a network of the same size, communication overhead is 40 bytes (explained in [14]). Thus, we can observe that the communication overhead of the proposed scheme is under considerable limits.

In the proposed scheme, computation overhead for pairwise secret keys assignment is very limited because of the use of combinatorial design based keys. Thus in the proposed scheme, the computation overhead is mainly due to MAC generation/verification. In the proposed scheme sensor nodes only submit the initial report to the CHs and CHs creates and attach MACs with the report. Moreover, the reports are forwarded only through CHs, thus MAC verification is done only by CHs. This helps in saving a lot of computation overhead from energy deprived sensor nodes.

### C. ENERGY REQUIREMENTS

False reports in the network can not only lead sink to take wrong decisions but also leads to extra energy consumption for forwarding such reports. Further, compromised sensor nodes can intentionally drop legitimate reports, leading to further energy wastage for sending same reports again. In this subsection, we identify the energy requirements for the proposed scheme. If $H$ represents average hops from source to sink, $e$ represents energy required by any intermediate sensor node for receiving and sending the report to next hop and $P$ represents the length of the report, then the energy requirements for a report where no en-route filtering is implemented can be given by,

$$E_{without} = H.P.e \tag{12}$$

in such a case all the reports whether correct or forged will travel all $H$ hops. When the proposed en-route filtering

scheme is implemented, correct reports travel all $H$ hops and false reports are dropped in maximum $h$ hops. Thus, energy requirement in such case can be given by,

$$E_{with\ en-route} = \{H(1-Z) + hZ\}.(P + L_{MCs} + L_{IDs}).e \tag{13}$$

where $Z$ is the percentage of false reports and $L_{MCs}$, $L_{ID}$ represents the length of MACs and key indexes respectively. This is the energy requirement for a report without selective forwarding attack. If we take into account the effect of selective forwarding attack, few correct reports can also be dropped before reaching the sink and such reports need to be sent again by the source. Thus finally, energy requirements for the proposed scheme can be given by

$$E_{with\ en-route} = \{H(1-Z) + h'(1-Z)P_{select}(X) + hZ\}. (P + L_{MCs} + L_{IDs}).e \tag{14}$$

where $P_{select}(X)$ represents the probability of dropping a report when $X$ CHs are compromised in the network and $h'$ represents average hops each correct report travels before being dropped by intermediate compromised CH. Moreover, energy consumption for computation is much less than communication, thus we only consider the energy consumed by communication of reports while calculating energy requirements for the network.

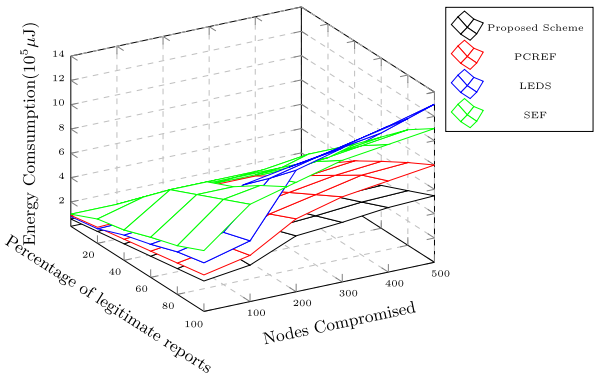


**FIGURE 9.** Energy Comparison in PCREF [14], LEDS [9], SEF [8] and the proposed scheme.

Experimental results for energy requirements for the whole network in the proposed scheme, SEF [8], LEDS [9] and PCREF [14] are given in Figure 9. In the figure, we can observe that LEDS [9] consumes maximum energy among the four compared schemes mainly because of poor filtering efficiency and because of broadcasting nature of the forwarded reports. SEF [8] performs better than LEDS because it do-not broadcast reports in each cell. PCREF [14] performs better than LEDS [9] and SEF [8] because of improved filtering efficiency. But energy requirements in PCREF [14] rises significantly with increased compromised sensor nodes. This is because of no preventive measures adopted by PCREF to restrict selective forwarding attack in the network, thus many correct reports can be dropped intentionally by intermediate sensor nodes and such reports are needed to be sent again by the source. The proposed scheme, on the other hand, has very high filtering efficiency and is highly resilient to report disruption and selective forwarding attacks, resulting in very low energy requirements in the network.

### D. NETWORK LIFETIME

Network Lifetime for a particular WSN can be defined as the duration of time for which the WSN can provide its basic requirements. In our scenario, network lifetime for a network can be defined as the time duration for which sensor nodes can sense the environment and create the reports, which then can be successfully forwarded through the multi-hops path to the sink.

In section V-C we discussed the energy requirements for the proposed scheme and we found that the proposed scheme has low associated energy consumption than SEF [8], LEDS [9] and PCREF [14]. Thus, the network lifetime for the proposed scheme is much more than SEF, PCREF and LEDS. Further, in the proposed scheme, we forward all the reports through cluster heads, which have more communication range than normal sensor nodes. Thus, in the proposed scheme, all reports travel fewer hops when compared with existing schemes, indirectly improving the network lifetime of the network.

## VI. CONCLUSION

In this article, we proposed a novel deterministic en-route filtering scheme based on combinatorial design. In the proposed scheme, the secret keys to CHs are assigned based on combinatorial design. We propose a novel beam model to further reduce key storage overhead in the network. When compared with existing deterministic en-route filtering schemes, the proposed scheme does not require reports to be sent through fixed paths. We observed that the filtering efficiency of the proposed scheme is much better than existing schemes such as SEF [8], PCREF [14], LEDS [9], LBRS [10], and IHA [15]. In the proposed scheme we proposed novel report generation, novel en-route filtering/sink verification methods. In the proposed scheme, each cell has three cluster heads and report forwarding/verification is only done by CHs. This helps in reducing the effect of selective forwarding attack while maintaining desired security in the network. It further reduces the energy requirements of the network. In the proposed scheme, three copies of each report with different endorsements are forwarded by the event cell towards the sink. This considerably improves data authenticity in the proposed scheme.

## REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.
[2] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, Jun. 2004.
[3] K. Xing and X. Cheng, "From time domain to space domain: Detecting replica attacks in mobile ad hoc networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[4] G. S. Kc, A. D. Keromytis, and V. Prevelakis, "Countering code-injection attacks with instruction-set randomization," in *Proc. 10th ACM Conf. Comput. Commun. Secur.*, 2003, pp. 272–280.
[5] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in *Proc. 1st Int. Conf. Embedded Netw. Sensor Syst.*, 2003, pp. 255–265.
[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, p. 13, 2011.
[7] M. Welzl, *Network Congestion Control: Managing Internet Traffic*. Hoboken, NJ, USA: Wiley, 2005.
[8] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 4, pp. 839–850, Apr. 2005.
[9] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 5, pp. 585–598, May 2008.
[10] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2005, pp. 34–45.
[11] C. Kraub, M. Schneider, K. Bayarou, and C. Eckert, "STEF: A secure ticket-based en-route filtering scheme for wireless sensor networks," in *Proc. 2nd Int. Conf. Availability, Rel. Secur. (ARES)*, Apr. 2007, pp. 310–317.
[12] H. Yang and S. Lu, "Commutative cipher based en-route filtering in wireless sensor networks," in *Proc. IEEE 60th Veh. Technol. Conf. (VTC-Fall)*, vol. 2, Sep. 2004, pp. 1223–1227.
[13] L. Yu and J. Li, "Grouping-based resilient statistical en-route filtering for sensor networks," in *Proc. INFOCOM*, Apr. 2009, pp. 1782–1790.
[14] X. Yang, J. Lin, W. Yu, P.-M. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, Jan. 2015.
[15] 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," in *Proc. IEEE Symp. Secur. Privacy*, May 2004, pp. 259–271.
[16] H. Harb, A. Makhoul, and C. A. Jaoude, "En-route data filtering technique for maximizing wireless sensor network lifetime," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 298–303.
[17] A. Kumar and A. R. Pais, "En-route filtering techniques in wireless sensor networks: A survey," *Wireless Pers. Commun.*, vol. 96, no. 1, pp. 697–739, 2017.
[18] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.
[19] S. Ruj and B. Roy, "Key predistribution using combinatorial designs for grid-group deployment scheme in wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 6, no. 1, p. 4, Dec. 2009.
[20] M. Akram and T. H. Cho, "Energy efficient fuzzy adaptive selection of verification nodes in wireless sensor networks," *Ad Hoc Netw.*, vol. 47, pp. 16–25, 2016.
[21] M. K. Shahzad and T. H. Cho, "Extending the network lifetime by pre-deterministic key distribution in CCEF in wireless sensor networks," *Wireless Netw.*, vol. 21, no. 8, pp. 2799–2809, 2015.
[22] S. A. Çamtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 15, no. 2, pp. 346–358, Apr. 2007.
[23] J. Lee and D. R. Stinson, "Common intersection designs," *J. Combinat. Des.*, vol. 14, no. 4, pp. 251–269, 2006.
[24] D. Chakrabarti, S. Maitra, and B. Roy, "A key pre-distribution scheme for wireless sensor networks: Merging blocks in combinatorial design," *Int. J. Inf. Secur.*, vol. 5, no. 2, pp. 105–114, 2006.
[25] A. Kumar and A. R. Pais, "A new hybrid key pre-distribution scheme for wireless sensor networks," in *Wireless Networks*. New York, NY, USA: Springer, 2018, pp. 1–15, doi: 10.1007/s11276-018-1698-z.
[26] S. Bag and B. Roy, "A new key predistribution scheme for general and grid-group deployment of wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, p. 145, 2013.
[27] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1984, pp. 335–338.
[28] A. Kumar and A. R. Pais, "A new combinatorial design based key pre-distribution scheme for wireless sensor networks," *J. Ambient Intell. Humanized Comput.*, pp. 1–16, 2018.
[29] I. Anderson, *Combinatorial Designs: Construction Methods*. Amsterdam, The Netherlands: Ellis Horwood, 1990.
[30] D. Stinson, *Combinatorial Designs: Constructions and Analysis*. New York, NY, USA: Springer-Verlag, 2007, doi: 10.1007/s12652-018-0902-4.
[31] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *Proc. 9th Annu. Int. Conf. Mobile Comput. Netw.*, 2003, pp. 81–95.
[32] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 54–69, Jul. 2005.
[33] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Lincoln, MA, USA: Ganga-Jamuna Press, 2006.
[34] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[35] F. Ye, G. Zhong, S. Lu, and L. Zhang, "Gradient broadcast: A robust data delivery protocol for large scale sensor networks," *Wireless Netw.*, vol. 11, no. 3, pp. 285–298, 2005.
[36] L. E. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*. Chelmsford, MA, USA: Courier Corporation, 2003.

**ALOK KUMAR** received the B.Tech. degree in computer science and engineering from Maharshi Dayanand University, India, and the M.Tech. degree in information security from Thapar University, India. He is currently a Research Scholar with the Department of Computer Science and Engineering, NITK Surathkal, India. His areas of interest include information security, network security, and wireless sensor networks.

**ALWYN R. PAIS** received the B.Tech. degree in computer science from Mangalore University, India, the M.Tech. degree in computer science from IIT Bombay, India, and the Ph.D. degree from NITK Surathkal, India. He is currently an Associate Professor with the Department of Computer Science and Engineering, NITK Surathkal. His areas of interest include information security, image processing, and computer vision.