A low-complexity, energy-efficient data securing model for wireless sensor network based on linearly complex voice encryption mechanism of GSM technology

M Saud Khan¹, Noor M Khan², Ahmad Khan¹, Farhan Aadil¹, M Tahir¹ and M Sardaraz¹

Abstract
A wireless sensor network is the formation of a temporary network of sensor nodes equipped with limited resources working in an ad hoc environment. Routing protocol is one of the key challenges while designing a wireless sensor network, which requires optimum use of limited resources of a sensor node, such as power and so on. Similarly, data security and integrity is another open issue that has emerged as a flash point in research community in the last decade. This article proposes a secure model for routing data from source to destination named as secure and energy-efficient routing. The proposed secure and energy-efficient routing is inherited from authentication and voice encryption scheme developed for Global System for Mobile Communications. Necessary modifications have been carried out in order to fit the Global System for Mobile Communications technology in a wireless sensor network ad hoc environment. Due to its low complexity, the secure and energy-efficient routing consumes lesser battery power both during encryption/decryption and for routing purposes. It is due to the XoR operation used in the proposed scheme which is considered as the most inexpensive process with respect to time and space complexity. It is observed through simulations that secure and energy-efficient routing can work effectively even in critical power level in a sensor network. The article also presents a simulation-based comparative analysis of the proposed secure and energy-efficient routing with two notable existing secure routing protocols. We proved that the proposed secure and energy-efficient routing helps to achieve the desired performance under dynamically changing network conditions with various numbers of malicious nodes. Moreover, in Global System for Mobile Communications, generally three linear feedback shift registers are used to fragment the key in data encryption mechanism. In this article, a mathematical model is proposed to increase the number of possible combinations of shift register in order to make the data encryption mechanism more secure which has never been done before. Due to its liner complexity, lesser power consumption, and more dynamic route updating, the secure and energy-efficient routing can easily find its use in the emerging Internet-of-Things systems.

Keywords
Wireless sensor network security, encryption, authentication, secure routing

Date received: 28 June 2020; accepted: 26 April 2021
Handling Editor: Yanjiao Chen

¹Department of Computer Science, COMSATS University Islamabad, Attock Campus, Islamabad, Pakistan
²Department of Electrical Engineering, Capital University of Science and Technology (CUST), Islamabad, Pakistan

Corresponding author:
Farhan Aadil, Department of Computer Science, COMSATS University Islamabad, Attock Campus, Islamabad 43600, Pakistan.
Email: Farhan.aadil@ciit-attock.edu.pk

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
Introduction

Wireless sensor network (WSN) is a self-configuring wireless network composed of either static or mobile nodes without any infrastructure (ad hoc mode) as shown in Figure 1. The sensor nodes in a network are equipped with a variety of functions, such as sensing, processing, aggregation, exchange of data, and so on. The size of a WSN may range from a few hundred to thousands of nodes depending on the requirement in the area of interest.

Energy efficiency and security are two major and all time open issues in WSN. Thus, a sensor node may die in relatively lesser time after its deployment if its operations are handled improperly. In other words, an energy-efficient node is the one whose operations consume minimum power during execution. Such operation includes routing, sensing, processing, authentication, and security. Apart from the usual operations that any sensor node has, such as, sensing, processing, and routing, security can be termed as a top-up for enhanced features.

This research mainly focuses on the use of WSNs in such hazardous areas, such as battlefield, fire zone, and so on, where security and energy efficiency are the issues of major concern. In a battlefield, various types of sensor nodes can be deployed like soldier trackers and acoustic sensors to monitor the approach of enemy while securing the parameters. Other extreme application is the fire zone where human access is not possible. Here, the sensor is mainly used for detecting life inside the building, taking the readings of fire and collecting building information.

Energy efficiency and security of data always remained as open research issues in WSN. Most of the battery power is consumed by routing of the data and thus the life of a network mainly depends on the efficiency of its routing protocol. The more the energy-efficient routing of a network, the longer will be its network lifetime. Moreover, the delivery of data to destination without being captured or forged by the attackers is also a vital issue. There are verities of protocols designed for energy-efficient routing and securing the data.

Rodoplu and Meng proposed an energy-efficient routing protocol. The technique is focused on the minimal use of power but requires the location information of each node through global positioning system (GPS) or other location techniques.

Chang and Tassiulas proposed a scalable cost-aware routing in WSNs. The “cost aware” refers to longer network life by choosing the optimum route having maximum residual energy. A new approach of routing based on renewable energy is proposed by Chalasani and Conrad known as energy-harvesting aware routing protocols. This technique proposes a mechanism to harvest the energy from external resources, such as energy from wind, solar, motion, noise and so on. However, this technique requires additional resources to be mounted over the node.

Moreover, another energy-harvesting awarded protocol is the distributed energy-harvesting aware routing algorithm (DEHAR), which describes a metric named as “energy distance” for selecting the optimum route. This metric calculates the route with minimum total energy distance instead of spatial distance. But this shortest energy distance is calculated by methods such as directed diffusion flooding which incurs routing overhead.

Beheshtiha et al. designed a routing protocol with energy-management functionalities known as opportunistic routing algorithm with adaptive harvesting–aware duty cycling (OR-AHaD). OR-AHaD is an opportunistic and adaptive protocol, which can dynamically tune the duty of a sensor node based on the remaining power in order to prolong its life in the network. The protocol however requires a regular update of energy levels and geographic information of a node. Moreover, the frequency of power updates increases with the passage of time as the power level of nodes decreases.

Another security protocol known as secure ad hoc on-demand distance vector (SAODV) is an extension of ad hoc on-demand distance vector (AODV). The protocol signs the data in SAODV to ensure the integrity of data. The mechanism used in SAODV known as double signature is used for authenticity but increases the processing overhead since signature on every chunk of data is an expensive process. To solve this limitation of SAODV, Cerri and Ghioni proposed another protocol known as A-SAODV. In A-SAODV, the nodes use request/reply mechanism like wireless networks. Reply to the request will be sent by a node only if it is not overloaded. Also, the replaying node can determine
whether to use single signature or double signature based on processing overhead. This mechanism is good in theory but again not suitable for resource-constrained WSNs.

Similarly, Zhou\textsuperscript{15} proposed an encryption and authentication–based protocol. The proposed scheme is named as routing protocol based on encryption and authentication (BEARP), which claims routing information confidentiality, authentication, and integrity of data. The idea of BEARP provides a good platform for data security in WSN; however, in WSN, the security and integrity of data never remained as a single and independent goal for the researcher. As discussed earlier, the network life and processing overhead, convergence time, network traffic, and so on are the challenges that arise while designing a secure routing protocol. The BEARP exchanges too many control messages, such as confidential data enquiry (CDE), routing path selection system (RPSS), confidential enquiry reply (CDER), confidential route reply (CRR), and acknowledgment. Even though all the communication between a base station (BS) and sensor nodes remains encrypted, still the BS adds a random number RB and a time stamp TB as an additional secure layer which obviously adds the processing overhead head to the nodes. The BEARP does not explain what is the probability of success and failure of the proposed scheme. Moreover, the paper lacks about the explanation what is the convergence/setup time of the proposed scheme.

Similarly, Djenouri et al.\textsuperscript{16} represent a secure ant colonization–based routing protocol. According to the paper, the proposed methodology has the capability of multilayer security threats; however, the term multilayer has not been explained clearly by the paper. The proposed methodology in the paper uses ant colony optimization and claims to achieve the security by four features: route discovery, route selection, route security, and data forwarding. The route is discovered by launching a broadcast request that reaches to a destination and the destination responds with an acknowledgment through backward broadcast. The path through which the packet arrives earlier is chosen as the shortest path. The watchdog algorithm is used to decide whether a packet needs to be secured before sending or not; if yes, the RC4 algorithm is used to encrypt the data. The paper does not explain how the RC4 algorithm is embedded with the proposed scenario also the probability of success or failure of secure model is also not highlighted.

The WSN faces the same security challenges as any ah-hoc network would.\textsuperscript{17,18} There are routing protocols that attempts to secure the network, such as TinySec,\textsuperscript{19} Spins,\textsuperscript{20} TinyPK,\textsuperscript{21} TinyECC,\textsuperscript{22,23} and LS-LEACH.\textsuperscript{24} The most popular technique in security domain of routing is the encryption and decryption of data. This technique is used to prevent or detect the unauthorized parties or malicious behavior of a sensor node. However, these solutions mostly run over application level resulting in a complex code implementation in higher-level language which adds processing overheads for a node’s processor. This phenomenon eventually fails the claim of secure and energy-efficient routing (SEER) protocol.

### Table 1. Types of attacks in WSN.

| Attack           | Mode    | Behavior                                                   |
|------------------|---------|------------------------------------------------------------|
| Sybil            | Active  | Reputation system is subverted by forging identities        |
| Dos              | Active  | Make the node to deny services by sending enormous number of packets |
| Sniffing         | Passive | Eavesdrops all the packets                                 |
| Tampering        | Active  | Change the routing packets                                 |
| Wormhole         | Active  | Often convince distant nodes that they are neighbors        |
| Sink hole        | Active  | Set the routing metrics to attract the nearby traffic       |
| Black hole       | Active  | A node starts to drop packets instead relaying it           |
| Gray hole        | Active  | Drop out some packets                                      |

### Attacks in WSNs

The data transmission services and network life both are solely dependent on routing protocols which makes them one of the most critical modules in the network. Usually the routing protocols are developed upon the assumption that sensing field is fully trustworthy and comfortable as far as the security is concerned. But this assumption does not come true in many situations. There are varieties of attacks that can be launched on a WSN. The most commonly discussed and launched attacks are Sybil, DoS, Sniffing, Tempering, Wormhole, Sinkhole, Black hole, Gray hole, and so on.\textsuperscript{25,26}

As shown in Table 1, these attacks can be categorized into active and passive attacks. In active attacks, a malicious sensor node may actively request sensitive information, or it can remove or change the messages transmitted over the network. Also, the active mode of attacks involves the ability to disturb the overall operation of the network, such as DoS. Whereas in passive...
attacks, a node intends to eavesdrop the transmission. The node in passive attack does not modify the data or inject its own packets to the network. The detection of passive attacker is difficult as compared to active attack.

Also, in active attacks, malicious nodes may gather sensitive information or behave selfishly in collaborative operations, such as routing, to passively affect the proper operation of WSNs. Table 1 summarizes the different types of attacks, their nature, and behavior.

A WSN is always prone to various types of attacks that can be launched to interfere in the operation and steal or forge data, such as wormhole, sinkhole, and Sybil attacks.27 The network once gained in such situation must also be able to prevent the attacker may start malfunctioning in various ways which must be monitored and isolated after detection.28

A design based on certificate-less signcryption for crowdsourced internet of things (IoT) based on the hyper elliptic curve is proposed by Ullah et al.29 Similarly, Waheed et al.30 proposed a new scheme namely known as N-PSC (new proxy signcryption) based on elliptic curve cryptography (ECC).

The sensor nodes once deployed mostly become vulnerable and inaccessible in hostile situation for the replacement of power source or other modules. Thus, in addition to securing data during routing, the nodes in such situation must also be able to prevent the wastage of energy in order to prolong the network life. The routing protocol must be able to select the optimum path for the routing of data to minimize the energy consumption. Thus, we have two objectives: energy efficiency and security of the data.

Most of the existing routing protocols can handle either energy efficiency or security of data at a time. Moreover, the security algorithms are mostly implemented as part of application layer causing additional cosmetics and overheads for processor, which at one side, although provides the security but consumes much more processing power at the other side. The routing protocol must balance the two objectives of energy and security by implementing the security algorithm at hardware level instead of its implementation at application level. To the best of our knowledge, such approach is not available in the literature.

**Contribution**

In this article, we propose a secure and energy-efficient scheme for routing data known as SEER, which not only provides end-to-end security of data but also strives to minimize energy consumption. The proposed scheme is designed to be implemented at hardware level to minimize the processing overhead and save battery power. We use GRACE routing protocol as a platform for the routing of data in an energy-efficient way. The simulation results show that the proposed security module is not only energy efficient but also provides a strong security against data interception attacks.

The proposed architecture introduces a low-complexity SEER mechanism by integrating A5 encryption scheme used for voice encryption in Global System for Mobile Communications (GSM).31 In this article, we introduced a secure version of GRACE routing protocol known as SEER. The proposed scheme is inherited from the voice encryption mechanism used in second-generation cellular mobile communication system, the GSM. The A5 algorithm is responsible for encrypting the voice data between the two parties. We implemented the A5 at hardware level which creates less computational burden over a sensor node. We embed the A5 algorithm in GRACE which is an energy-efficient routing protocol.

One of the beauties of A5 algorithm is that we can create a key for encryption of any length. Thus, the proposed scheme can support the data packet of 32, 64, and 128 bits. The proposed routing protocol can be

| Pseudo code for secure and energy-efficient routing |
|-----------------------------------------------|
| The following are the terminologies used in the given algorithm: |
| $\gamma$ : is a 19 bits binary key |
| $\Omega$ : is 22 bits binary key |
| $\psi$ : is a 23 bit binary key |
| $K_c$ represents the output key used as a session key for data encryption |
| $\beta$ : is the length (number of bits) of the output key |
| $\psi$ : used as an operator to add new bits to the current vector |
| RAND is a 128 bit key received from base station |
| $K_i$ is a 128 bit key stored in the node |
| $S = RAND_{1,64} \oplus RAND_{65,128} \oplus RAND_{65,128}$ |
| $(K_i, 64 \oplus K, 65, 128)$ |
| $\gamma \leftarrow S_{1,19} \Omega \leftarrow S_{21,41} \psi \leftarrow S_{42,64}$ |
| $\text{epoch} \leftarrow 1, \beta \leftarrow 16$ |
| $\alpha \leftarrow \text{model}(\gamma_9, \Omega_{10}, \psi_{10})$ |

**For each epoch $< \beta$ do**

| $b \leftarrow \gamma_{16} \oplus \gamma_{17} \oplus \gamma_{18} \oplus \gamma_{19}$ |
| $\text{shift } \gamma \text{ one bit right and append } b \text{ to the left}$ |
| **end** |
| $\text{If } \Omega_{10} = \alpha \text{ then}$ |
| $b \leftarrow \Omega_{21} \oplus \Omega_{22} \oplus \Omega_{21} \oplus \Omega_{22}$ |
| $\text{Shift } \Omega \text{ one bit right and append } b \text{ to the left}$ |
| **end** |
| $\text{If } \psi_{10} = \alpha \text{ then}$ |
| $b \leftarrow \psi_{9} \oplus \psi_{9} \oplus \psi_{9} \oplus \psi_{9}$ |
| $\text{Shift } \psi \text{ one bit right and append } b \text{ to the left}$ |
| **end** |
| $K_c \leftarrow K_c \oplus \beta$ |
| **end** |

$$Data_{\text{enyp}} \leftarrow K_c \oplus Data_{\text{sensing}}$$
implemented both at centralized as well as hierarchical sensor networks depending on the needs and requirements. Simulations are performed to validate the performance of the proposed algorithm in MATLAB (version 8.61). From the simulation results, we prove that the proposed scheme is not only secure enough to protect the data but also requires lesser processing and battery power as compared to notable existing data securing schemes. Also, the proposed scheme consumes lesser convergence time to become ready for exchange of data. Moreover, the scheme creates little message overhead resulting in negligible increase in the traffic of the network. In order to prove the efficiency, the performance of the proposed algorithm is compared with the two mentioned secure routing protocols that is, Gong et al.33 and Alrajeh et al.34 Second, we devised a mechanism to perturb the length of shift registers in variable number unlike GSM which uses only three fixed shift registers named as X, Y, and Z registers. We developed probabilistic models to prove the strength of the proposed mechanism. To the best of our knowledge, this novel work has never been done before.

**Working of A5 algorithm used in GSM**

As discussed earlier, the A5 encryption procedure is originally designed for second-generation GSM-based networks. This mechanism is responsible for the confidentiality of voice data between the parties. The subscriber identity module (SIM) contains the ciphering key-generating algorithm, the A8 algorithm. The A8 algorithm is used to calculate the 64-bit ciphering key $K_c$ which is used to encrypt the voice data before it is sent over a channel. The ciphering algorithm A5 ensures the secure communication between the mobile station (MS) and the network. The GSM network initiates a request and sends it to MS over the control channel.

The MS is first authenticated through signed response using A3 algorithm. After successful authentication, the following steps are carried out in order to incorporate voice encryption mechanism:

- The MS receives a random number RAND from the BS as a challenge.
- The MS generates a key known as Session Key $K_c$.
- This session key is produced by using the A8 algorithm, the subscriber authentication key $K_i$ is assigned to each MS, and the random challenge RAND.
- The MS sends the session key $K_c$ to the BTS.
- Meanwhile, the mobile services switching center also produces and sends its session key $K_c$ to the BS.
- The BS receives the session key $K_c$ from the mobile services switching center and the MS and compares them to verify its authenticity.
- The BS verifies the session keys received from the MS and the mobile services switching center.

The voice encryption algorithm A5, as explained in Figure 2, is then initialized with the verification of the Session Key $K_c$.

The A5 encryption scheme uses three shift registers in the processor: X, Y, and Z. The values assigned to these registers are as follow:

- X: 19 bits (X0, X1, X2,..., X18) first 19 bits of $K_c$ loaded to X.
- Y: 22 bits (Y0, Y1, Y2,..., Y21) next 22 bits loaded to register Y.
- Z: 23 bits (Z0, Z1, Z2,..., Z22) last 23 bits loaded to register Z.

Figure 3 represent the execution of process inside a processor. After the bits are shifted to the respective registers, a majority rule is applied to elect the successor. For this purpose, bits from position X8, Y10, and Z10 are picked from X, Y, and Z registers, respectively. The majority rule picks two successors based on bit 1 or bit 0. The position having maximum numbers of 1s or 0s will become successor like in our example, the
register X and register Z are the successors, as there are two 1s and one 0.

In the next step, the two registers (X and Z) are stepped forward. In register X, the positions 13, 16, 17, and 18 are taken and XorRed with each other. The result is saved at least significant bit (LSB) by shifting the register values to right side.

Similarly, from the Z register, the bits from positions 7, 20, 21, and 22 are picked and XorRed with each other, saving the result at LSB.

The proposed SEER scheme

Data encryption algorithm for proposed SEER

**SEER Algorithm.** In order to implement the A5 encryption mechanism in WSN, we make necessary modifications in the existing encryption/decryption scheme implemented in GSM. Figure 4 depicts the block diagram of proposed scheme. The data security mechanism can then be used in both ad hoc network environments. In ad hoc mode, a sink is responsible to encrypt/decrypt the data sent by a source node. The step-by-step procedure of the proposed algorithm is given below:

- The BS generates a 128-bit random challenge known as RAND.
- RAND is forwarded to the sensor nodes as a challenge in order to authenticate it.
- The sensor node starts to calculate the session key $K_i$ with the help of A8 and $K_i$.
- The algorithm A8 and the key $K_i$ is already provided to the node.
- The BS also starts to calculate the session key $K_c$.
- The sensor node sends $K_c$ to the BS, CH, sink, or server.
- The BS receives the $K_c$ and matches it with its own produced $K_c$.
- If both the $K_c$’s are the same, it means the communicating nodes is a valid node, else the $K_c$ is discarded and node iD is black listed.
- The data are sent encrypted over air interface.

Figure 5 illustrates a distributed network with hierarchical structure having Cluster Heads (CHs) along with the member sensor nodes. We assume that the CH to be a powerful node that may become a sink in case of a centralized network and are directly connected to gateway or BS. The malicious Nodes are assumed to be present in the network and they have the complete information of security mechanism of the network. The CH is responsible to convey encrypted data transmitted from low powered sensor nodes present in its vicinity to sink, gate way or BS. The CH sends the report of any malicious activity to the BS or any controlling entity if determined. Although only one BS is shown in figure but there could be as many BS as required by the network and environment. The deployment of nodes can be Arial or manual depending upon the nature of physical environment. Each sensor node is assigned an ID and the position of the sensor node is assumed to be known to it. We also assume that the sink or cluster
head has all the necessary information about member sensor nodes, such as sensor ID, sensor MAC address, and the assigned authentication key $K_i$.

**Probability of interception.** We derived the following probabilistic model in order to prove the strength of the proposed model against the interception attempts. The following parameters are focused:

- Probability of random number generation of $n$ size.
- The probability of splitting the key into $D$ number of group registers.
- The probability of selecting a random bit from each of these $D$ group registers and its exploitation in $l$ possible binary operations.
- The probability of perturbation process.

Let $i$ be the length of random generated binary keys. Thus, there are $2^n$ different keys. The probability to generate a particular key $K_i$ of $i$th node is given by

$$P(K_i\text{generation}) = \frac{1}{2^n}$$

We split the key $K_i$ into $D$ distinct integral parts of lengths $n_1, n_2, n_3, ..., n_d$ such that

$$\sum_{d=1}^{D} n_d = n$$

where $n_d$ is the length of the $d$th part of $K_i$ with the condition that

$$1 < n_d < n - 1$$

In order to distribute the key $K_i$ with the condition that

![Figure 4. Block diagram of data encryption/decryption in WSN.](image1)

![Figure 5. Hierarchical WSN.](image2)
The probability to split a key $K_i$ of length $n$ into $D$ different keys is given by

$$P(\text{groupkey}) = \frac{1}{C_n} = \frac{1}{\left[ \frac{D-1}{d-1} \right]^d \sum_{i=0}^{n} \binom{n}{i}}$$

Thus, the probability to generate a valid key is given by

$$P(\text{valid key}) = P(\text{Kc generation}) \cdot P(D \text{ distant group key generation}) \cdot P(\text{bits selection}) \cdot P(\text{perturbation})$$

$$= \frac{1}{2^n} \cdot \frac{1}{C_n} \cdot \frac{1}{\prod_{i=1}^{D-1} \left( \frac{n - 2D + d}{d} \right)} \sum_{i=0}^{\frac{n}{2^n}} \binom{n}{i} \cdot \frac{1}{\prod_{i=1}^{D-1} \left( \frac{n - 2D + d}{d} \right)}$$

$$= \frac{1}{2^n} \cdot \frac{1}{C_n} \cdot \frac{1}{\prod_{i=1}^{D-1} \left( \frac{n - 2D + d}{d} \right)} \sum_{i=0}^{\frac{n}{2^n}} \binom{n}{i} \cdot \frac{1}{\prod_{i=1}^{D-1} \left( \frac{n - 2D + d}{d} \right)}$$

**Vulnerability level of interception of session key ($K_c$) when multiple registers are used**

As discussed earlier, the proposed SEER algorithm uses the A5 algorithm for encryption. In this process, the session key ($K_c$) is divided into three linear feedback shift registers. The use of three fixed shift registers can be compromised easily in the presence of powerful malicious nodes. We proposed a mechanism to proceed the data encryption process by increasing the number of shift registers. The number of possible combinations of registers must be in odd number to fulfill the condition of majority functions as discussed in section C.

The vulnerability level of interception of interception for the proposed scheme is given below

$$P_b = \frac{1}{C_b}$$

where $P_b$ represents the level of vulnerability or interception and $C_b$ represents the total number of possible combination of bits if the key.

We derived a formula to produce the total number of possible odd combinations of registers after increasing the number of registers from three registers to a possible odd number, keeping the length of the session key $K_c$ constant.

As we know that the total possible combinations depend on two factors, that is, number of distinct registers and length of the key. We represent the statement as

$$C_b = P_1 P_2$$

where $P_2$ represents the length of the key depends on $n$ (number of bits of session key ($K_c$)) and independent of $D$ distinct register. Thus, it is a binomial mutation with formulation

$$P_2 = \sum_{i=0}^{n} \binom{n}{i}$$

where as $P_1$ is a product of multiple terms that depend on the variable $d$ which ranges from 1 to $D-1$. The value of $D$ cannot be equal to 2, and also there must be more than two bits in each register. In other words, we have the equation

$$\left( \frac{n - dD + d}{d} \right)$$

where $D$ is the number of distinct registers that can take values 3, 5, 7, and 9. $d$ is the index that starts from 1 and goes up to $D-1$ values.

Thus, $P_1$ becomes

$$P_1 = \left[ \prod_{d=1}^{D-1} \frac{n - 2D + d}{d} \right]$$
The total number of combinations of $n$-bits encryption key is shifted in $D$ distinct registers and is given by the formula

$$C_b = \left[ \prod_{d=1}^{D} \frac{n - 2D + d}{d} \right] \times \left[ \sum_{i=0}^{n} \binom{n}{i} \right]$$

**Proof by example.** Taking the simplest scenario. Suppose we have number of registers $D = 3$.

The total numbers of bits in a session key ($K_c$) is $n = 8$.

By substituting the values we get

$$C_b = \left[ \frac{8 - 6 + 1}{1} \times \frac{8 - 6 + 2}{2} \right] \times \left[ \binom{8}{0} + \binom{8}{1} + \binom{8}{2} + \ldots + \binom{8}{8} \right]$$

We get $6 \times 256 = 1536$.

Hence, the vulnerability level of interception of breaking 8-bit session key segregated in the three registers becomes

$$P_b = \frac{1}{1536} = 6.5 \times 10^{-4}$$

This example shows that by increasing the number of registers, the total number of combinations will also increase. This means that when bits’ combinations increase, the vulnerability level of intercepting the data decreases; or in other words, there will be less chances for the interceptor to get the session key. As far as the relationship of the vulnerability level of interception with the number of registers is concerned, by increasing the number of registers, the number of combinations of bits increases and the vulnerability level of interception decreases. In other words, with an increase in the number of combinations, the vulnerability level of interception decreases, and our data are more secure and protected.

**Results and discussion**

The performance of the proposed SEER mechanism is evaluated through different parameters, such as number of alive nodes, energy consumed by the sensor nodes, traffic overhead, packet delivery ratio and end-to-end delay. Extensive simulations have been carried out for the evaluation purpose using a simulation scenario of 500 nodes deployed randomly in 100 m × 100 m area. The simulation was run multiple times to obtain average results for the aforementioned parameters. The obtained results are then compared with the two notable secure routing protocols ETRAP and SRCE.

Figure 6 shows the lifetime comparison of SEER with SRCE and ETRAP. As discussed earlier, SRCE is an energy-harvesting protocol; thus, the nodes harvest energy from an external source during its operation. Therefore, the number of alive nodes of SRCE is greater than the SEER and ETRAP. However, the SEER still outperforms and stays longer even in extreme sensing environment. However, if SRCE is run without energy-harvesting module, its lifetime curve falls much faster than SEER and ETRAP as shown in the figure. Figures 6 and 7 depicts the energy consumed by each sensor node when SRCE runs without an energy-harvesting module. The total energy consumed by individual sensor node includes data packet formation, route selection, routing table, data security mechanisms, and data routing. However, more energy may be consumed in procedures specific to protocol.
Figure 8 represents a traffic overhead comparison of the three protocols. The comparison is done in terms of number of packets exchanged between nodes and the BS or gateway. These messages include control overheads, data packets, acknowledgments, and so on. The figure shows that ETRAP has a great traffic overhead as compared to SRCE and SEER. Both SRCE and SEER give almost similar result till the number nodes reach to 400 where the trend of the plot seems to be different. The plot shows a clear change when the number of nodes reaches to 450 where the similarity of SEER and SRCE performance begin to break.

Figure 9 shows the packet delivery ratio in the presence of malicious nodes. The presence of malicious nodes deeply affects the performance of a network. This may lead the network to degrade its packet delivery. The figure shows a comparative analysis packet delivery ratio of SEER in comparison with ETRAP. This result has been taken in the presence of a variable number of compromised or malicious nodes. As we can see, that ETRAP has a very rapid fall in throughput with the number of increased malicious nodes. SEER and SRCE, however, provide a better result against the initial number of compromised nodes as can be seen in the result. There is a slight fall in both SEER and SRCE in the malicious nodes between 40 and 50, but SEER again provides a constant and satisfactory data rate as compared to SRCE.

Figure 10 shows the end-to-end delay of data among the nodes. The delay is calculated as the time taken by
the protocol to take a packet from source to destination. This delay also includes the time taken by the node to place a bit on the medium after being encrypted. It has been observed that the SEER has the lowest end-to-end delay among all. This is because, the GRACE by its self has a fast mechanism for selecting the most optimum route before transmitting the data and adds less overhead to it than other ETRAP and SRCE. Since the SEER is designed to work at hardware level, it adds comparatively less overhead resulting a minimum end-to-end delay.

Conclusion

In this article, we proposed a secure mechanism for routing protocol known as SEER protocol. The proposed protocol is based on A5 encryption scheme developed for GSM. SEER has been tested through simulations in MATLAB by setting up hostile and vulnerable WSN scenarios with respect to data integrity. The obtained results were than compared with other two notable secure routing protocols. We proved that the proposed SEER helps to achieve the desired performance under dynamically changing network conditions with various number of malicious nodes. Due to its liner complexity, lesser power consumption and more dynamic route updation, SEER can easily find its use in the emerging IoT systems.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.
Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs
Noor M Khan https://orcid.org/0000-0002-6118-3790
Ahmad Khan https://orcid.org/0000-0002-6955-8876
Farhan Aali https://orcid.org/0000-0001-8737-2154
M Tahir https://orcid.org/0000-0002-7750-8959
M Sardaraz https://orcid.org/0000-0002-7169-8683

References
1. Zaman N, Jung LT and Yasin MM. Enhancing energy efficiency of wireless sensor network through the design of energy efficient routing protocol. J Sens 2016; 2016: 9278701.
2. Chang WL, Zeng D, Chen RC, et al. An artificial bee colony algorithm for data collection path planning in sparse wireless sensor networks. Int J Mach Learn Cyber 2015; 6(3): 375–383.
3. Sisinni E, Depari A and Flammini A. Design and implementation of a wireless sensor network for temperature sensing in hostile environments. Sens Actuat A: Phys 2016; 237: 47–55.
4. Bokde ND, Peshwe PD, Gupta A, et al. RemoteWSN; a novel technique for remotely visualizing connectivity in WSN working on a weight based routing algorithm. In: Recent advances in electronics & computer engineering (RAECE), Roorkee, India, 13–15 February 2015, pp.92–95. New York: IEEE.
5. Kuthadi VM, Selvaraj R and Marwala T. An enhanced security pattern for wireless sensor network. In: Satapathy SC, Srujan Raju K, Mandal JK, et al. eds) Proceedings of the second international conference on computer and communication technologies. New York: Springer, 2016, pp.61–71.
6. Hameed K, Saleem Khan M, Ahmed I, et al. A zero watermarking scheme for data integrity in wireless sensor networks. In: 197th International conference on network-based information systems (NBIS), Ostrava, 7–9 September 2016, pp.119–126. New York; IEEE.
7. Naz P, Hengy S and Hamery P. Soldier detection using unattended acoustic and seismic sensors. In: Proceedings SPIE 8389, ground/air multisensor interoperability, integration, and networking for persistent ISR, Baltimore, MD, 24 May 2012. Bellingham, WA: SPIE.
8. Rodoplu V and Meng TH. Minimum energy mobile wireless networks. IEEE J Select Area Commun 1999; 17(8): 1333–1344.
9. Chang JH and Tassiuas L. Energy conserving routing in wireless ad-hoc networks. In: INFOCOM 2000 nineteenth annual joint conference of the IEEE computer and communications societies, Tel Aviv, 26–30 March 2000, pp.22–31. New York; IEEE.
10. Chalasani S and Conrad JM. A survey of energy harvesting sources for embedded systems. In: IEEE Southeastcon, Huntsville, Al. 3–6 April 2008, pp.442–447. New York: IEEE.
11. Jakobsen MK, Madsen J and Hansen MR. DEHAR: a distributed energy harvesting aware routing algorithm for ad-hoc multi-hop wireless sensor networks. In: IEEE international symposium on world of wireless mobile and multimedia networks (Womom), Montreal, QC, Canada, 14–17 June 2010, pp.1–9. New York; IEEE.
12. Beheshthia SS, Tan HP and Sabaei M. Opportunistic routing with adaptive harvesting-aware duty cycling in energy harvesting WSN. In: 15th international symposium on wireless personal multimedia communications (WPMC), Taipei, 24–27 September 2012, pp.90–94. New York: IEEE.
13. Lu S, Li L, Lam KY, et al. SAODV: a MANET routing protocol that can withstand black hole attack. In: International conference on computational intelligence and security, Beijing, China, 11–14 December 2009, pp.421–425. New York: IEEE.
14. Cerri D and Ghioni A. Securing AODV: the A-SAODV secure routing prototype. IEEE Commun Mag 2008; 46(2): 120–125.
15. Zhou J. Efficient and secure routing protocol based on encryption and authentication for wireless sensor networks. Int J Distrib Sens Netw 2013; 9(4): 108968.
16. Djenouri D, Khelladi L and Badache N. A survey of security issues in mobile ad hoc networks. IEEE Commun Surv 2005; 7(4): 2–28.
17. Zhou L and Haas ZJ. Securing ad hoc networks. IEEE Network 1999; 13(6): 24–30.
18. Stajano F and Anderson R. The resurrecting duckling: security issues for ubiquitous computing. Computer 2002; 35(4): 22–26.
19. Karlof C, Sastry N and Wagner D. TinySec: A layer link security architecture for wireless sensor networks. In: Proceedings of the 2nd international conference on embedded networked sensor systems, Sensys ’04, Baltimore, MD, 3–5 November 2004, pp.162–175. New York: ACM.
20. Perrig A, Szewczyk R, Tygar JD, et al. SPINS: security protocols for sensor networks. Wirel Netw 2002; 8(5): 521–534.
21. Watro R, Kong D, Cuti SF, et al. TinyPK: Security sensor networks with public key technology. In: Proceedings of the 2nd ACM workshop on security of Ad Hoc and sensor networks, SASN ’04, 25 October 2004, pp.59–64. New York: ACM.
22. Liu A and Ning P. TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks. In: International conference on information processing in sensor networks (ipsn 2008), St. Louis, MO, 22–24 April 2008. New York: IEEE.
23. Fenn HW and Rachmarini D. A secure routing protocol for wireless sensor networks with consideration of energy efficiency. In: 2012 IEEE network operations and management symposium, Maui, HI, 16–20 April 2012, pp.105–112. New York: IEEE.
24. Alshowkan M, Elleithy K and Alhassan H. LS-LEACH: a new secure and energy efficient routing protocol for wireless sensor networks. In: IEEE/ACM 17th international symposium on distributed simulation and real time applications, Delft, 30 October–1 November 2013, pp.215–220. New York: IEEE.
25. Yu Y, Li K, Zhou W, et al. Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. *J Netw Comput Appl* 2012; 35(3): 867–880.

26. Sun YL, Han Z, Yu W, et al. A trust evaluation framework in distributed networks: vulnerability analysis | defense against attacks. In: *Proceedings IEEE INFOCOM 2006. 25th IEEE international conference on computer communications*, Barcelona, 23–29 April, pp.1–13. New York: IEEE.

27. Towle JP, Herold D, Johnson R, et al. Low-cost acoustic sensors for littoral anti-submarine warfare (ASW). In: *SPIE 6538, Sensors, and Command, Control, Communications, and Intelligence*, Orlando, FL, 9–12 April 2007. Bellingham, WA: SPIE.

28. Karlof C and Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Netw* 2003; 1(23): 293–315.

29. Ullah I, Ul Amin N, Zareei M, et al. A lightweight and provable secured certificateless signcryption approach for crowdsourced IoT applications. *Symmetry* 2019; 11: 1386.

30. Waheed A, Umar A, Zareei M, et al. Cryptanalysis and improvement of a proxy signcryption scheme in the standard computational model. *IEEE Access* 2020; 8: 131188–131201.

31. Global system for mobile www.gsma.com (accessed on 2 February 2019).

32. Khan NM, Khalid Z and Ahmed G. GRAdient cost establishment (GRACE) for an energy-aware routing in wireless sensor networks. *EURASIP J Wireless Commun Netw* 2009; 15: 275694.

33. Gong P, Chen TM and Xu Q. ETARP: an energy efficient trust-aware routing protocol for wireless sensor networks. *J Sens* 2015; 2015: 469793.

34. Alrajeh NA, Khan S, Lloret J, et al. Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks. *Int J Distrib Sens Netw* 2013; 9: 374796.