An Secured and Energy Conserved Utilization Path Algorithm using Secret Key and Adaptive Partition Controller in WSN

K.Ramanan* and E.Baburaj**
* Deparment of Computer Science & Engineering, Sathyabama University chennai, India
ramana3483@gmail.com
** Department of Computer Science & Engineering, Sun College of Engineering,Nagercoil, India
alanchybabu@gmail.com

Abstract: In wireless sensor networks (WSNs), secured and energy conserved data gathering are two important performance metrics for critical event monitoring in wireless sensor networks. Current state-of-the-art research is limited to either maximizing security under redundant radix-based approach or security through adversary model while satisfying throughput requirement. Although many prior research efforts resulted in optimized solutions, but how to optimize both objectives simultaneously has to be addressed. Our proposal work aimed on presenting an integrated configuration called Secret Key and Adaptive partition controller (SK-APC) is to maximize the fastness of data gathering of sensed data in the sink. To focus on secure data gathering of sensed data events, the encryption and decryption of sensor data is simplified using Keyed Hash Function. We show that the solution to the integrated configuration problem characterizes the secured energy conserved data gathering through XORing operations. Next, an Adaptive partition controller based on minimum Steiner tree is presented with the objective of reducing the energy consumption of sensed data gathering at the sink. By applying the minimum Steiner tree, minimum hops between source and sink nodes are identified satisfying the energy conservation principal. An extensive simulation analysis to demonstrate the security aspect and energy conservation principal with time taken for data gathering is presented. The obtained results show that SK-APC provides comparatively better performance than the state-of-the-art works in terms of both security and energy efficiency. Experimental analysis shows that SK-APC is able to reduce the time for data gathering by 25.72% and energy consumption by 18.48% compared to the state-of-the-art works.

Keywords: Energy conserved, data gathering, radix-based approach, Keyed Hash Function, Adaptive partition controller, Minimum Steiner tree.

Introduction

Current Improvement in communication have resulted in a significant shift in wireless sensor network research and as a result a secured and energy conserved data gathering configuration is the need of the hour. Many research works have been contributed in this aspect.

Protection Location Privacy in Wireless Sensor Network (PLP-WSN) [1] covered. Redundant Radix-based Approach (RRA) [2] in Wireless Sensor Network (WSN) provided an energy conserved means of communication using hybrid approach called Frequency Shift Keying (FSK) and Amplitude Shift Keying (ASK). Similar approaches to realizing Energy Efficient Routing protocols in WSN are found in [3] [4]. However, all the above mentioned methods lack an integrated effort in ensuring security and energy efficiency of data being collected, which is the core objective of our configuration.

The topological Structure in Layered Configurations (TSLC) [23] is a routing algorithm based on range of WSN which is used to perform the data communication. It is saves the energy of the entire network efficiently. In addition, it also increases the quality of the network service performance, and extends the life cycle of the network. Based on the communication protocol, it fails to realize the network energy protection. It also explains performance of throughput as well as the end-to end delay.

Recently, many data aggregation approaches using privacy homomorphism encryption have been presented and analyzed on wireless sensor networks. The approach in [5] used Recoverable Concealed Data Aggregation (RCDA) in WSN while in [6] a Routing algorithm to increase the lifetime of the network using Data Gathering Scheme (DGS) was presented to ensure data integrity and improving network lifetime. However, both the approaches lack data aggregation rate while exchanging messages between source and sink node. Data aggregation rate is addressed in the configuration SK-APC by applying Keyed Hash Function.

Energy-Efficient and Relay Hop Bounded Mobile Data Gathering Algorithm (BRH-MDG) [24] is established where the data collecting latency is effectively reduced by performing local aggregation through multihop transmissions. Then, the

algorithm uploads the data aggregated to the mobile collector. But, the BRH-MDG algorithm is failed in energy utilization of the entire network optimized. Discrete Cosine Transform (DCT) [26] of compactness attribute is used in sensory data and it is also used to improve the recovery accuracy. The time complexity of the algorithm is evaluated in the DCT method for reducing the computational cost. But, the realistic sensor signal is not accurately sparse. Thus, the low sampling rate causes insufficient measurements and fails in accuracy recovery.

Related works

A wireless sensor network comprises of thousands of small sensors with non rechargeable batteries. For such sensor nodes, the energy consumption during transmission is much more than during computation. Hence such networks employ Energy Efficient and High Accuracy [7] model for data aggregation. Cluster based data gathering [8] to ensure efficient data transmission was presented.

Location-Energy Spectral Cluster Algorithm (LESCA) [21] is determined in many clusters in a network. The spectral classification is providing on location-energy using the residual energy in various network nodes. The Location-Energy Spectral performance is improves the energy efficiency and also increased network lifetime. The clustering algorithms are not handled in an optimal method. So, the entire energy consumed of sensor network per round gets increased rapidly.

Energy Efficient Cluster Based Scheduling Scheme [22] for wireless sensor networks maintains the network lifetime, increases power as well as the high delivery ratio. Ubiquitous wireless connectivity was established in [9] with the objective of improving network lifetime. A resource aware algorithm [10] ensured location privacy while extending network lifetime. Though network lifetime and energy efficient approaches were ensured there observed a tradeoff in terms of time for data gathering which is addressed in the configuration SK-APC using Adaptive partition controller.

Energy-Efficient Adaptive Routing [27] is produced the energy load on multiple routes and it performs the quality of the network lifetime with increasing the end-to-end transmission. However, the energy efficiency is reduced because energy efficiency frequently fetches the additional latency. Secure and reliable routing protocols for WSNs [28] are estimated to handle the application of security requirements and the reliable data transmission using selective encryption method. However, protocol sending more data over the multipath is required in order to recognize a certain number of path failures.

There are several performance hurdles that hamper the design and deployment of WSN during critical monitoring applications. In [11], Latin Squares were adopted to ensure low packet delay and low overhead. However, network lifetime with respect to scalability with which the data packet can be transmitted remained unsolved. To improve network lifetime Eigen Beam forming was applied in [12] ensuring security in fading channels. Energy analysis component for quality of protection- modeling language (QoP-ML) [25] evaluated the inclined of many security stages on the energy utilization of a protocol. However, components fail to consider the trade-off between security and energy efficiency.

While various investigations have been carried out in the direction of energy efficient data gathering in WSN [13] [14] [15] security while data being collected at the sink remains to be explored. In particular, with appropriate encryption and decryption of sensor data, it may be possible to be extended to address security aspect.

Numerous critical monitoring applications like commercial and military require secure operation of sensor networks, and the outcome is affected largely with highly compromised sensor nodes in the network. Similar approaches employing energy efficient and security in WSN are found in [16] [17] [18]. But the rate at which data integrity was provided remained unaddressed, which is addressed in SK-APC by reducing the false positive data aggregate rate using Symmetric Key and Cyclic Redundancy Check. The approach in [19] uses Cyclic Diversionary Routing (CDR) while in [20] Energy Based Connected Dominated Set was used to improve security increasing the lifetime of network.

The movable and deployable resource unit[29] (MDRU)-based network provides communication services in disaster-struck areas where the lack of spectrum and energy resources is intensified due to the high demand from users and the power outages after a disaster. The MDRU-based network attempts to apply spectrum- and energy-efficient methods to provide communications services to users. A novel data collection scheme, called the Maximum Amount Shortest Path[30] (MASP), that increases network throughput as well as conserves energy by optimizing the assignment of sensor nodes. MASP is formulated as an integer linear programming problem and then solved with the help of a genetic algorithm. A two-phase communication protocol based on zone partition is designed to implement the MASP scheme. We also develop a practical distributed approximate algorithm to solve the MASP problem. In addition, the impact of different overlapping time partition methods is studied.

A good energy conserved and secured data gathering configuration should resolve energy imbalance while improving the security with respect to data being collected at the sink in WSN. Motivated by this, we investigate an integrated configuration to realize the objective that secured and energy conserved data gathering is efficiently provided. The main contributions of this paper are as follows. Secured data gathering configuration to reduce the false positive data aggregate rate at the sink node in WSN is proposed, in which a Marvin Keyed Hash Function, used to enhance the fastness of data gathering in the sink node. Construction of Steiner tree to minimize the energy consumption is designed.

The remainder of the paper is organized as follows: Secured Energy Efficient Data gathering configuration is given in Section 2, the Secret Key and Adaptive partition controller (SK-APC). The programming model and implementation with experimental setup is presented in Section 3, the implementation and numeric experimental results with discussions are shown in Section 4. The concluding remark is provided in Section 5.

Secret Key and Adaptive partition controller

In this work, a Bi-criteria optimization problem, to maximize security while minimizing energy consumption in improving the fastness of the data gathering of the sensed data event in the sink is presented. Figure 1 shows the block diagram of the Secret Key and Adaptive partition controller (SK-APC) configuration.

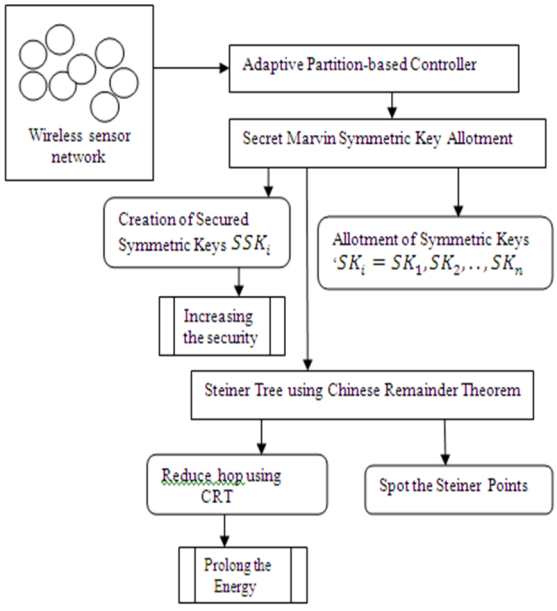

Figure1. Block diagram of Secret Key and Adaptive partition controller (SK-APC)

Fig. 1 shows that, the configuration SK-APC is divided into two parts. With the objective of improving the security, Secret Marvin Symmetric Key Allotment is applied to the sensor nodes in WSN for the sensed data event. Secret Marvin Symmetric Key Allotment model first performs an efficient distribution of Symmetric Key by performing XOR operations and likelihood function. Next, aiming at conserving the energy, a Steiner Tree using Chinese Remainder Theorem is applied that observes the steiner points (i.e., center node or sink node) and reduce the hop by applying CRT. As a result, a secured energy efficient data gathering on wireless sensor network is established.

Representation of Secret Marvin Symmetric Key Allotment

In this module, the representation of Secret Marvin Symmetric Key Allotment is increasing the security is presented. The SK-APC configuration uses a Secret Marvin Symmetric Key Allotment model for data being collected. The Secret Marvin Symmetric Key Allotment model is divided into three steps: Symmetric Key Allotment, discovering Symmetric Key and Route-Symmetric Key generation. The three steps in the design of SSKG model are described briefly as follows.

Let us assume that each sensor node '$SN_i = SN_{1,} SN_{2,.....,} SN_n$' in Wireless Sensor Network (WSN) is assigned with a Symmetric Key '$SK_i = SK_1, SK_2, .., SK_n$' $SK_i = SK_{1,} SK_{2,.....} SK_n$ that is disclosed only to the sink node 'S' and is mathematically formulated as given below.

$$\sum_{i=1}^{n} SN_i \rightarrow SK_i \rightarrow S \qquad (1)$$

From (1), the sensor nodes in WSN include a Symmetric Key and only with the help of this Symmetric Key, the sensor communicates with the sink node. This Symmetric Key 'SK_i' used to encrypt sensor data and generate Keyed Hash Function for each sensor data. In order to achieve security, the SK-APC configuration uses Keyed Hash Function that instead of using

the Symmetric Key 'SK_i' directly, each sensor node obtain a Error Detecting Code (EDC) to generate Secret Symmetric Key 'SSK_i'.

During encryption, for 'j' sensor data, using EDC, source node generates an '$i-j$' Frame Check Sequence and the resulting frame of 'j' sensor data divisible by predetermined threshold value is used. On the other hand during decryption by the sink node, the incoming sensor data frame is divided by the predetermined threshold value.

This Secret Symmetric Key 'SSK_i' is then XORed (i.e., encrypted) with the sensor data in addition to the EDC and is formulated as given below.

$$Encrypted_{SD} \sum_{i=1}^{n} SSK_i \; XOR \; SD_i \tag{2}$$

The Secret Symmetric Key 'SSK_i' are generated by applying a threshold, 'δ' left padded with 'n' sensor data bits and is mathematically formulated as given below.

$$\sum_{i=1}^{n} SSK_i \rightarrow \delta \ll n \tag{3}$$

In this method, a large Symmetric pool of 'n' Keys are first generated using the Symmetric Key Allotment. The second step is the discovering of Symmetric Key where each sensor node in WSN locates which of its nearby sensor node shares the common key with itself by exchanging discovery messages between the sensor nodes.

During the successful accomplishment of discovering common key, a secured link is established between them, ensuring security and reducing false positive data aggregates. Fig.2 shows the diagrammatic representation for discovering symmetric key by the sensor nodes (i.e., 10 sensor nodes). The figure shows two different types of arrows where dotted arrow represents successful discovering of symmetric key between the sensor nodes whereas the dashed arrow specifies the discovering of symmetric keys through multi-hop sensor nodes.

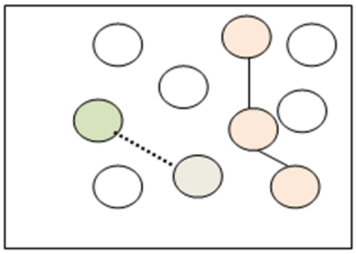

Figure 2. Symmetric key discovering

The Route-Symmetric Key generation step, an end-to-end Route Symmetric Key is assigned to pair neighbor nodes which do not share a common Symmetric Key. These sensor nodes in the SK-APC configuration are then linked by multi-hop secure links at the end of discovering of Symmetric Key. At the end of the Route-Symmetric Key generation, the likelihood that any pair of sensor nodes possesses at least one Symmetric Key is given as below

$$Likelihood\ (SN_i) = \frac{((SSK_i - n)!)^2}{(SSK_i - 2n)! * SSK_i!} \tag{4}$$

The above Secret Marvin Symmetric Key Allotment model, secure routing is performed from a source sensor node to the sink node. The security mechanism for data gathering of the sensed data event is based on the Marvin Keyed Hash Function.

The Marvin Hash Function Symmetric Key (MHF-SK) algorithm for data gathering for sensed data event is given as follows (in Fig. 3). The design of MHF-SK algorithm involves two steps. The two step process involves the encryption and decryption of sensor data to improve the fastness of data Gathering of sensed data event in the sink node, with the aim of increasing the security.

As shown in Fig. 3 ,the design of MHF-SK algorithm, involving efficient encryption and decryption aiming at improving the security of data gathering for sensed data event (i.e., data packet) by the sink node. In order to perform encryption, Symmetric Key and Secret Symmetric Key are obtained for each sensor nodes. Based on these two keys, the source node which wants to send the sensor data senses the presence of the neighbor nodes with same Symmetric Key.

```
Input: Let Sensor Node be 'SN_i = SN_1, SN_2, ..., SN_n', Symmetric Key
  'SK_i = SK_1, SK_2, .., SK_n',  sink node 'S', Sensor Data SD_i
Output: Secured Data Gathering at sink node
Begin
For each Sensor Node SN_i
    If SN_i wants to send SD_i
        Assign with a symmetric key SK_i
        Evaluate Secret Symmetric Key 'SSK_i' using (3)
        If neighbor Sensor Node SN_i identified with SK_i
            Perform XORing (i.e., encryption) with the sensor data using (2)
            else
            Evaluate likelihood using (4) to identify multi hop sensor nodes
        End if
            If sink node 'S' received Sensor Data SD_i from SN_i
            extract Sensor Data SD_i from SN_i
            Perform XORing (i.e. decryption)
        End if
    End if
End for
End
```

Figure 3. Marvin Hash Function Symmetric Key (MHF-SK) algorithm

On detection, an XOR operation is performed with efficient data gathering at the sink node. On the other hand, if neighboring nodes with same Symmetric Key is not detected, then the likelihood is measured to identify the multi-hop sensor nodes. In this similar manner, data gathering at the sink node is performed in a highly secured manner. One the other hand, decryption process is applied to extract the sensor data using the XORing operation. In this way, security for data being collected at the sink node is ensured. The next section discuss in detail about the energy conservation principal.

Representation of Steiner Tree

This model, we define an Adaptive Partition-based Controller based on Steiner Tree for energy efficient data gathering in WSNs. The aim of this model is to increase the percentage of sensor data successfully transferred, while reducing the energy consumption of sensor nodes. Let us consider a graph '$G = (V, E)$'where 'G' contains all the source nodes SN_i and sink 'S' respectively.

The aim of improving the energy efficiency, the SK-APC configuration uses Adaptive partition controller based on Minimum Steiner Tree that initially pairs up the available source nodes 'SN_i'and then randomly selects a hub node (i.e., center node or the Steiner point) from the node-pair. On the other hand, the loads of the non-hub node are shifted to the hub node, assigning the transmission costs on that specific edge. As a result, the non-hub node is removed and the hub node with aggregated load is grouped as a new set of sources. This process is repeated until the sink node is the only remaining node in the entire network. Fig.4 shows the Steiner Tree representation for four sensor nodes.

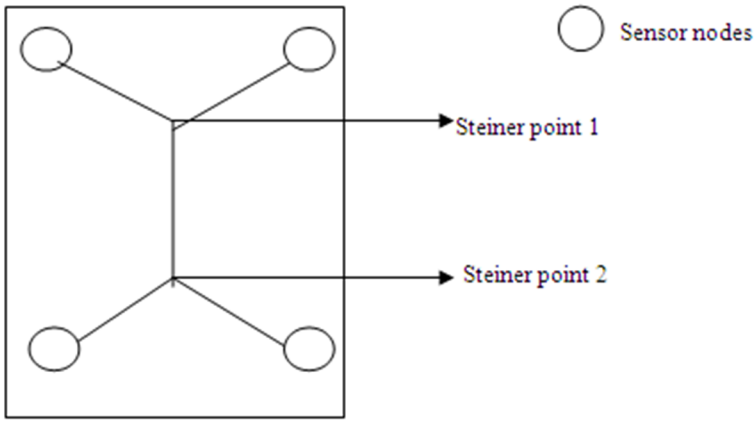

Figure. 4 Representation of Steiner Tree for four sensor nodes with two steiner points

The above-stated energy efficient task definitions, the energy efficient data gathering and successful sensor data transfer is maximized while reducing the energy usage by deciding upon the next hop that can be used as the forwarders (i.e., forwarding sensor nodes). After the formation of Steiner Tree the SK-APC configuration moves forward with the aid of Chinese Remainder Theorem (CRT) for splitting the sensor data packets.
Let us consider 'R' primes where '$r_i > 1$' then consider the product which is given as below

$$M = \Pi_i r_i \tag{5}$$

From (5) 'M' represents the multiplicative sensor data that produces simultaneous congruences and is obtained as below

$$m = \sum_{i=1}^{n} (coeff_i * m_i) \tag{6}$$

According to the CRT, the SK-APC configuration alternatively identifies with the set of numbers 'm_i' provided that 'r_i' are known. In addition, the CRT in the SK-APC configuration applies an Adaptive partition controller that instead of 'm' uses the mathematical formulation as given below

$$m_i = \sum_{i=1}^{n} [m_i * mod(r_i)] \tag{7}$$

By applying the above formulation, the maximum energy consumed by each sensor node for data gathering of the sensed data event in the sink node is reduced substantially.

Experimental Discussion

In this section we present the numerical data obtained as a result of applying SK-APC. Table 1 lists the set of input parameter and evaluates performance of SK-APC via simulation. Our example WSN consists of 100 sensor nodes deployed in a square area of A^2 (1600 m * 1600 m) placed in a random manner in the wireless sensor network that generates traffic for every 10 m/s.
The nodes are distributed in an area using Random Way point model for simulation, whereas the link layer provides the link between two nodes and the design of link is multi direction. The radio ranges are dynamically adjusted between 5m and 40 m to maintain network connectivity. The sink node collects the data packets of range 8 – 56 and forwards the data to the sink node with each data packet size differing from 100 KB to 512 KB. The simulation time varies from 5000 simulation seconds to 1600 simulation seconds.
Omni directional antenna is used for simulation and at any instant of time only single process is performed (i.e., either packet transmission or packet reception). Let us assume that the transmission color purple is selected as a starting point with a moving speed of 30 m/s and ends at anywhere in the network area. The default color for each sensor node is set and also the shape for each node is set by declaring variable m1 and assigned it with three shapes circle, hexagon and square. Communication is performed between the sensor nodes if the frequency matches between them and lies within its communication range.

Table 1. Simulation Parameters

Parameters	Values
Network area	1600 m * 1600 m
Number of sensor nodes	10,20,30,40,50,60,70,80,90,100
Number of data packets i.e., size of data block	9,18,27,36,45,54,63,72
Range of communication	40 M
Speed of node	0 – 30m/s
Simulation time	1600 s
Number of runs	8

Result and Discussion

In this section the result analysis of SK-APC is made and compared with two existing methods, Protection Location Privacy in Wireless Sensor Network (PLP-WSN) [1] and Redundant Radix-based Approach (RRA) [2] in WSN. The nodes in SK-APC configuration are positioned in uniform topology. To evaluate the efficiency of SK-APC, the following metrics like security, energy consumption, execution time for data gathering and data aggregate rate in Wireless Sensor Network is measured.

Impact of Security for data gathering

Security with respect to data being collected is measured on the basis of data packets received at the sink node in WSN. Therefore, security is the difference between the total packets sent to the packets not received at the sink node.

$$S\,(DC) = Packets_s - Packets_{nr} \tag{8}$$

Table 2. Security for data gathering with respect to hop count

Hop Count	Security for data gathering (p/s)		
	SK_APC	PLP_WSN	RRA
2	131	117	99
4	134	119	102
6	138	123	105
8	143	125	107
10	147	128	108

From (8), '$Packets_s$' refers to the data packets sent and '$Packets_{nr}$' refers to the data packets not received at the sink node in WSN. It is measured in terms of packets per second (p/s). The values obtained through (8) is tabulated for different hop count using the proposed SK-APC configuration and compared elaborately with the existing two works PLP-WSN [1] and RRA [2] respectively.

Fig. 5 shows the security for data collected at the sink node with respect to different hop counts. To better perceive the efficacy of the proposed SK-APC configuration, substantial experimental results are illustrated in Figure 5 and compared against the existing PLP-WSN [1] and RRA [2] respectively. The results reported above confirm that with the increase in the number of hop counts in WSN, the data collected at the sink node also increases and comparatively observed to be higher using SK-APC. So, the configuration SK-APC is said to be secured than compared to PLP-WSN and RRA. From the table 2, with a hop count of 2, 130 data packets (i.e., p/s) were efficiently collected at the sink node using the SK-APC configuration, whereas 117 and 99 packets per seconds were collected at the sink using PLP-WSN and RRA. The data packets collected at the sink is improved with the application of Secured Symmetric Key Distribution model. With the objective of improving security, Secured Symmetric Key Distribution model performs an XOR operation with the sensor data packet in addition to the Error Detecting Code (EDC). As a result, the successful packets received using SK-APC is improved and therefore security is improved by 9.77% compared to PLP-WSN and 23.33% compared to RRA.

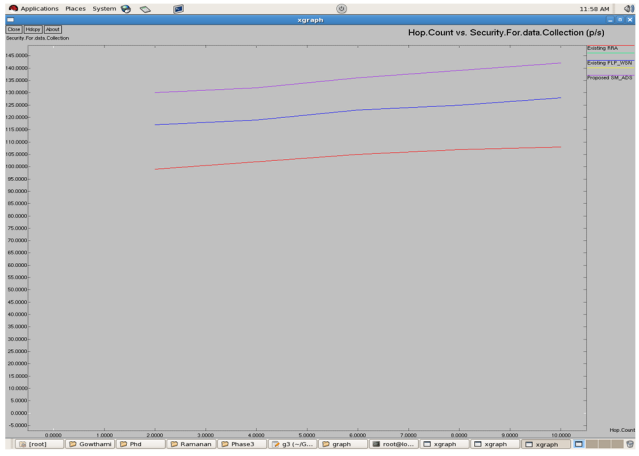

Figure 5. Measure of security for data gathering with respect to hop count

Impact of False Positive Data Aggregate rate

Whenever sensor nodes in the network send data, due to the presence of misbehaving nodes in WSN, possibility of packet drops occur during data packet transmission, that inject the false data into the packet and send to sink node. Then sink node then collects that packet. As a result, false positive data gets aggregated at the sink node. False positive data aggregate rate is the ratio of false data aggregated at the sink node to the overall data packet in WSN. The false positive data aggregate rate is formulated as given below

$$FPDA = \frac{False\ data\ packet}{Overall\ data\ packet} * 100 \quad (9)$$

From (9), ‘’, the false positive data aggregate rate for different number of sensor nodes in the range of 10 to 70 is measured.
In the experimental setup, the number of sensor nodes ranges from 10 to 70. The results of seven simulation runs conducted to measure the false positive data aggregate rate are listed in table 3. As listed in table 3, the SK-APC measure the false positive data aggregate rate which is measured in terms of percentage (%). The false positive data aggregate rate obtained using our configuration SA-ADS offer comparable values than the state-of-the-art methods.
The targeting results of false positive data aggregate rate using SK-APC configuration is compared with two state-of-the-art methods PLP-WSN and RRA and figure 6 is presented for visual comparison based on the relevant information. The figure shows the false positive data aggregate rate with respect to sensor nodes, with each sensor nodes sending different data packets to the sink node. As illustrated in figure 6, when 10 sensor nodes sent data packet to the sink node, the false positive data aggregate rate using SK-APC configuration was 21% compared to PLP-WSN and RRA that showed 27% and 25% respectively. Our configuration SK-APC differ from the ACSDTP differs from the PLP-WSN and RRA in that we have incorporated Marvin Keyed Hash Function. The advantage of applying using Keyed Hash Function in SK-APC configuration is that instead of using the Symmetric Key directly, each sensor node obtains a Error Detecting Code (EDC) to generate Secret Symmetric Key. This Secret Symmetric Key are then used for the communication between sensor and sink node which reduces the false positive data rate by 29.16% compared to PLP-WSN and 21.15% compared to RRA.

Table 3. False Positive data aggregate rate with respect to sensor nodes

Sensor Nodes (N)	False Positive data aggregate rate (%)		
	SK_APC	PLP_WSN	RRA
10	23	27	25
20	27	32	29
30	29	34	31
40	30	35	32
50	31	37	34
60	32	38	36
70	36	40	38

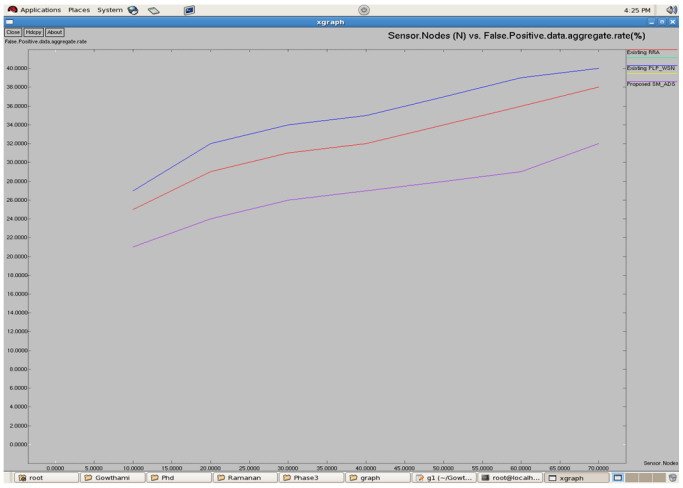

Figure 6. Measure of false positive data aggregate rate

Impact of Energy consumption for data gathering

Energy consumption for data being collected at the sink node is the product of energy consumed by a single sensor node and the total sensor nodes in WSN.

$$EC = Energy_{sn} * Total_{sn} \quad (10)$$

From (10), 'EC' is the energy consumption for data gathering at the sink node whereas 'sn' represents the sensor nodes. The consumption of energy is measured in terms of Joules.

Table 4. Energy consumption with respect to sensor nodes

Sensor Nodes (N)	Energy Consumption (Joules)		
	SK_APC	PLP_WSN	RRA
10	47	58	64
20	51	60	66
30	53	61	69
40	54	64	70
50	56	65	72
60	60	67	73
70	62	69	75

In Table 4 we further compare the energy consumed by different number of sensor nodes for data gathering at the sink in WSN. The experiments were conducted using seventy sensor nodes and the energy consumed is measured in terms of Joules (J).

Fig. 7 given above shows the energy consumption rate for SK-APC configuration, PLP-WSN [1] and RRA [2] versus seventy different sensor nodes. The energy consumption returned over SK-APC configuration increases gradually though not linear for differing sensor nodes when compared to the two other methods. From figure 7, it is illustrative that the energy consumption for the data being collected at the sink node is reduced using the proposed SK-APC configuration This is because with the application of Steiner tree based on the minimum number of hops being selected between source and sink nodes, the energy consumption is reduced. The Steiner tree with the aid of Chinese Remainder Theorem split the sensor nodes data packets that decide the next hop to be selected as the forwarding nodes. Only after the selected forwarding nodes sensor nodes data packets are sent that reduces the energy consumption of data being collected at the sink node by 13.08% compared to PLP-WSN and 23.89% compared to RRA respectively.

Impact of time for data gathering

Time taken for data gathering is the difference between the end time and start time for data gathering by the sink node in WSN. It is measured in terms of milliseconds and is formulated as given below.

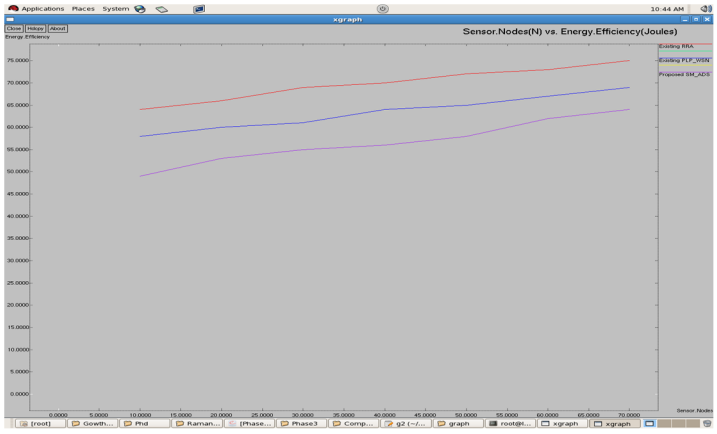

Figure 7. Measure of energy consumption

$$DC_t = (Endtime_{DC} - Starttime_{DC}) \qquad (11)$$

Table 5. Time Taken Data Gathering With Respect To Sensor Nodes

Sensor Nodes (N)	Time taken for Data gathering (ms)		
	SK_APC	PLP_WSN	RRA
10	124	173	185
20	142	177	197
30	154	182	201
40	158	191	216
50	171	198	221
60	173	209	224
70	192	215	227

From (11), the time for data gathering is measured using 'DC_t', whereas '$Endtime_{DC}$' represents the end time for data gathering by the sink node and '$Starttime_{DC}$' represents the start time for data gathering by the sink node in WSN. Table 5 shows the time for data gathering with respect to 70 sensor nodes with a moving speed of 25 m/s. To better perceive the efficacy of the proposed SK-APC configuration, substantial experimental results are illustrated in Figure 7 and compared against the existing PLP-WSN [1] and RRA [2] respectively.

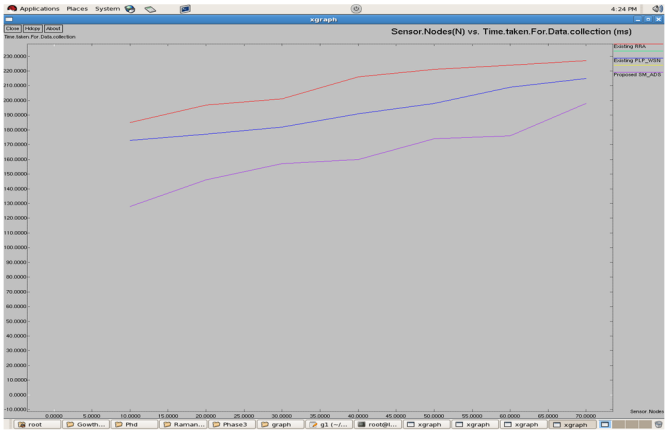

Figure 8. Impact of Time taken for data gathering

Fig. 8 shows the impact of time taken for data gathering with respect to varying sensor nodes in the range of 10 to 70 and the time for data gathering using three methods differs according to the size of sensor nodes. The results reported above confirm that with the increase in the number of sensor nodes being sent to the sink node for data gathering, the time for data gathering also increases. From figure 8, the time for data gathering using three methods differs according to the size of sensor nodes. As illustrated in Figure, the proposed SK-APC configuration performs relatively well when compared to two other methods PLP-WSN [1] and RRA [2]. This is because of the application of Adaptive Partition-based Controller randomly selects a hub node from the node pair. As a result, the loads of the non-hub node are shifted to the hub node. The non-hub node is removed and the hub node with aggregated load is grouped as a new set of sources. Through this, the time taken for data gathering using the SK-APC configuration is reduced by 21.86% compared to PLP-WSN and 29.58% compared to RRA respectively.

Conclusion

This article presents a novel configuration Secured Marvin and Adaptive Partition-based Controller (SK-APC) using the Marvin Keyed Hash Function. The performance of the proposed configuration is compared with secured data gathering and energy efficient data gathering methods (namely, PLP-WSN and RRA). The proposed configuration has the following advantages. (i) Improves security for data being collected at the sink node, (ii) provides low false positive data aggregate rate, (iii) representation of Steiner tree for achieving the energy conservation principle. The security in SK-APC configuration is improved using Secured Marvin Symmetric Key Distribution that applies Symmetric Key and Secret Symmetric Key during encryption and decryption that is available only to the source and sink node. By applying Marvin Keyed Hash Function and CRS, the false positive data aggregate rate is reduced significantly. Finally with the construction of steiner tree, the energy consumption for data gathering at the sink node is reduced considerably. Simulations were conducted to measure the performance of SK-APC configuration and evaluated the performance in terms of different metrics, such as security, false positive data aggregate rate, energy consumption and time to perform data gathering at the sink node in WSN. The results show that SK-APC configuration offers better performance with an improvement of security by 16.55% and reducing the false positive data aggregate rate by 25.15% compared to PLP-WSN and RRA respectively.

References

[1] Kiran Mehta, Donggang Liu, and Matthew Wright,," Protecting Location Privacy in Sensor Networks against a Global Eavesdropper", IEEE Transactions on Mobile Computing, Vol. 11, No. 2, February 2012.

[2] Koushik Sinha, Bhabani P. Sinha, and Debasish Datta," An Energy-Efficient Communication Scheme for Wireless Networks: A Redundant Radix-Based Approach", IEEE Transactions On Wireless Communications, Vol. 10, NO. 2, February 2011.

[3] Manish Kumar Jhaa, Atul Kumar Pandey, Dipankar Pala, Anand Mohan," An energy-efficient multi-layer MAC (ML-MAC) protocol for wireless sensor networks", International Journal of Electronics and Communications (AEÜ), Elsevier, Mar 2010.

[4] Jalel Ben-Othman, Bashir Yahya," Energy efficient and QoS based routing protocol for wireless sensor networks, J. Parallel Distrib. Comput, Elsevier, Mar 2010.

[5] Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin, and Hung-Min Sun," RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 4, April 2012.

[6] Yi-hua Zhu, Wan-deng Wu, Jian Pan, Yi-ping Tang," An energy-efficient data gathering algorithm to prolong lifetime of wireless sensor networks", Computer Communications, Elsevier, Jan 2010.

[7] Hongjuan Li, Kai Lin, Keqiu Li," Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks", Computer Communications, Elsevier, Mar 2010.

[8] Hongbo Jiang, Shudong Jin, and Chonggang Wang," Prediction or Not? An Energy-Efficient Framework for Clustering-based Data Collection in Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Volume:22 , Issue: 6, Apr 2011.

[9] Ahmad Rahmati, and Lin Zhong," Context-Based Network Estimation for Energy-Efficient Ubiquitous Wireless Connectivity",IEEE Transactions On Mobile Computing, Vol. 10, No. 1, January 2011.

[10] Chi-Yin Chow, Mohamed F. Mokbel and Tian He," A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks",IEEE Transactions On Mobile Computing, Vol. 10, No. 1, January 2011.

[11] Chih-Kuang Lin, Vladimir I. Zadorozhny, Prashant V. Krishnamurthy, Ho-Hyun Park, and Chan-Gun Lee," A Distributed and Scalable Time Slot Allocation Protocol for Wireless Sensor Networks", IEEE Transactions On Mobile Computing, Vol. 10, No. 5, April 2011.

[12] Xiangyun Zhou, Radha Krishna Ganti and Jeffrey G. Andrews," Secure Wireless Network Connectivity with Multi-Antenna Transmission",IEEE Transactions On Wireless Communications, Vol. 10, No. 2, February 2011.

[13] Anfeng Liu, Laurence T. Yang, Motoki Sakai, andMianxiong Dong," Secure and Energy-Efficient Data Collection in Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013.

[14] Anfeng Liuyz , Zhongming Zhengz , Chao Zhangy, Zhigang Cheny, and Xuemin (Sherman) Shenz, " Secure and Energy-Efficient Disjoint Multi-Path Routing for WSNs", Volume:61 , Issue: 7, Sep 2012.

[15] Kamlesh A. Waghmare, Dr. P.N. Chat," Energy Efficient Data Collection and Routing Algorithm in Wireless Sensor Network: A Survey", International Journal For Research In Emerging Science And Technology, Volume-1,Issue-2, July-2014.

[16] Sung Jin Choi, Kyung Tae Kim, and Hee Yong Youn," An Energy-Efficient Key Predistribution Scheme for Secure Wireless Sensor Networks Using Eigenvector", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013.

[17] Jiliang Zhou," Efficient and Secure Routing Protocol Based on Encryption and Authentication for Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013.
[18] Chaoran Li and Yun Liu," ESMART: Energy-Efficient Slice-Mix-Aggregate for Wireless Sensor Network", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013.
[19] Ju Ren, Yaoxue Zhang, and Kang L," An Energy-Efficient Cyclic Diversionary Routing Strategy against Global Eavesdroppers in Wireless Sensor Netwo", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013.
[20] Xiaoyan Kui, Yu Sheng, Huakun Du, and Junbin Liang," Constructing a CDS-Based Network Backbone for Data Collection in Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013.
[21] Ali Jorio, Sanaa El Fkihi, Brahim Elbhiri, and Driss Aboutajdine "An Energy-Efficient Clustering Routing Algorithm Based on Geographic Position and Residual Energy for Wireless Sensor Network" Hindawi Publishing Corporation Journal of Computer Networks and Communications Volume 2015, Article ID 170138, 11 pages.
[22] E. Srie Vidhya Janani1 and P. Ganesh Kumar "Energy Efficient Cluster Based Scheduling Scheme for Wireless Sensor Networks" Hindawi Publishing Corporation The Scientific World Journal, Volume 2015, Article ID 185198, 9 pages.
[23] Jun Yu and Xueying Zhang "A Cross-Layer Wireless Sensor Network Energy-Efficient Communication Protocol for Real-Time Monitoring of the Long-Distance Electric Transmission Lines" Hindawi Publishing Corporation Journal of Sensors Volume 2015, 13 pages.
[24] Ling Chen, JianxinWang, Xiaoqing Peng, and Xiaoyan Kui, "An Energy-Efficient and Relay Hop Bounded Mobile Data Gathering Algorithm in Wireless Sensor Networks" Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2015, 9 pages.
[25] Damian Rusinek, Bogdan Ksiezopolski, and Adam Wierzbicki "Security Trade-Off and Energy Efficiency Analysis in Wireless Sensor Networks" Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2015, 17 pages.
[26] Kefu Yi, Jiangwen Wan, Tianyue Bao, and Lei Yao "A DCT Regularized Matrix Completion Algorithm for Energy Efficient Data Gathering in Wireless Sensor Networks" Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2015, 11 pages.
[27] Shaohua Wan "Energy-Efficient Adaptive Routing and Context-Aware Lifetime Maximization in Wireless Sensor Networks" Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2014,16 pages.
[28] Hind Alwan and Anjali Agarwal "A Multipath Routing Approach for Secure and Reliable Data Delivery in Wireless Sensor Networks" International Journal of Distributed Sensor Networks,Volume 2013 (2013),10pages.
[29] T. Ngo; H. Nishiyama; N. Kato; T. Sakano; A. Takahara," A Spectrum Energy- Scheme for Improving the Utilization of MDRU-Based Disaster Resilient Networks",IEEE Transactions on Vehicular Technology,Year:2014,Volume:63,Issue:5,Pages:2027-2037.
[30] S.Gao;H.Zhang;S.K.Das,"Efficient Data Collection in Wireless Sensor Networks with Path Constrained Mobile Sinks",IEEE Transactions on Mobile Computing,Year:2011,Volume:10,Issue:4,Pages:592-608.