Securing Sensor Networks by Moderating Frequencies

Pinaki Sarkar[1(✉)], Priyatosh Mahish[2], Morshed Uddin Chowdhury[3], and Kouichi Sakurai[4]

[1] Department of Mathematics, Techno India University, Kolkata, West Bengal, India
pinakisark@gmail.com
[2] Department of Electrical Engineering, NIST, Berhampur, Odisha, India
priyatosh.priyo@gmail.com
[3] School of Information Technology, Deakin University, Melbourne, VIC, Australia
morshed.chowdhury@deakin.edu.au
[4] Department of Informatics, Kyushu University-Ito Campus, Fukuoka, Japan
sakurai@csce.kyushu-u.ac.jp

Abstract. Security of Wireless Sensor Network (WSN) is a key issue in information security. Most existing security protocols exploit various Mathematical tools to strengthen their security. Some protocols use the details of the geographical location of the nodes. However, to the best authors' knowledge, none of the existing works exploit the constraints faced by the adversary, specifically, tracing a particular frequency from a large range of unknown frequency channels. The current work uses positional details of the individual nodes. Then the aim is to exploit this weakness of tracing frequencies by assigning a wide range of frequency channels to each node. Experiments using Magneto Optic Sensors reveal that any change of the parametric Faraday's rotational angle affects the frequency of the Optical waves. This idea can perhaps be generalized for practically deployable sensors (having respective parameters) along with a suitable key management scheme.

Keywords: Security of wireless sensor networks · Key management schemes · Radio frequency channels · Magneto-optic sensors · Faraday's rotational angle

1 Introduction

The modern generation demands secure transmission of information at a low cost. Thus, security of low cost networks like Wireless Sensor Networks (WSN) have become an important area of study. Such distributed networks consist of numerous identical low cost devices called nodes or sensors along with one or a few powerful Base Stations (BS), connecting the network to the user. The standard method of incorporating hierarchy in such networks is by introducing relatively powerful special nodes called Cluster Heads (CH). For instance, the

J. Tian et al. (Eds.): SecureComm 2014, Part II, LNICST 153, pp. 173–185, 2015.
DOI: 10.1007/978-3-319-23802-9_15

works [6,16] implements a hierarchy to the classic Transversal Design ($TD(k,p)$) based Key Predistribution Scheme (KPS) [8].

Most existing key management schemes in the literature of WSN concentrate on strengthening their design by the use of Mathematical tools. There are some protocols like [16] which consider the location of the nodes. However, not many, according to the authors' knowledge, have exploited the difficulties faced by the adversary. The main philosophy behind the current work is to exploit the practical hazards faced by the adversary while trying to retrieve the encrypted message. For retrieving any message *encrypted* by the application of a suitable key management protocol and being transmitted in open wireless (Magneto Optical) medium, the attacker primarily does the following:

1. Identify the frequency channels on which the message is being transmitted.
2. Decrypt the encrypted message passing through those frequency channels.

Till date, nodes of a given sensor network are normally configured with specific *frequency channels* or *frequency bands*. The authors suggest preallocating different sensors with varied sets of frequency channels. Of course, for direct communication between any two such sensors preloaded with two distinct sets of (multiple) frequency bands, there should be at least one common band between them. Such a suggestion is certainly practical and cost effective. For instance, mobile phone handsets with multi-Sim card are available at a reasonable price. These handsets generally use different set of frequency channels for different geographical locations (usually for different countries). This justifies the (practical) proposal of manufacturing (numerous) low cost sensor nodes preallocated with different sets of frequency bands.

Once sensors having different frequency channels are available, each node can be preloaded with certain small number ($\mathbf{n}$) of channels out of a large number ($\mathbf{N}$) of channels meant for the entire network. The adversary may easily trace the entire range of channels for a network. However tracing the exact frequency channels for individual nodes may still be difficult. The concept will be detailed in Sect. 2.

Considering this practical hazard faced by an adversary, the focus shift towards investigating whether the transmission frequencies can be regulated within the nodes; perhaps based on certain parameter(s). For this, experiments have been conducted with Magneto Optic sensors depending on Faraday's Magneto optic effect. The results are plotted in Fig. 2 of Sect. 5. Though such sensor may not suit specific security purpose, the success of the experiments suggest the same can be expected of other application specific sensors with respect to the variations of their respective parameters.

1.1 Related Works

Constraint in resources among the nodes of any WSN generally restricts the use of computationally expensive public key during encryption of messages. Instead, the use of relative inexpensive symmetric key cryptography is preferred. Symmetric key cryptography demands the communicating parties to share the same

(or easily derivable) keys prior to message exchange. This emphasizes the importance of adequate key management schemes for such networks. Key Predistribution Schemes (KPS) consisting of preloading the keys before deployment and establishing these symmetric keys immediately afterwards are considered to be one of the best possible management techniques for such networks. Most of the first generation KPS are random in nature which has been well briefed in an excellent technical report [5] authored by Çamtepe and Yener. The same authors initiated the trend of deterministic KPS through their pioneering work [4]. Wei and Wu [17] and Lee and Stinson [7] independently came up with deterministic proposals at almost the same time. The work [17] deduces the general conditions for any scheme to be optimal in terms of connectivity, resilience and memory usage while analyzing existing KPS, and in the process proposes two schemes that can achieve their deduced optimality criteria. The works [7,8,11] establishes that deterministic schemes are better suited than their random counterparts for key establishment post deployment. This motivates the proposal of various deterministic KPS. An updated survey of such schemes can be traced in [11] and the references therein.

Ren *et al.* [12] proposes a location-aware end-to-end security framework in which each node only stores a few secret keys. These secret keys are determined by the node's geographic location. The property of the location-aware keys successfully limits the impact of compromised nodes to their vicinity. Multifunctional key management framework ensures both node-to-sink and node-to-node authentication along with report forwarding routes. Their one-to-many data delivery approach guarantees efficient en-route bogus data filtering and is robust against many known DoS attacks. However since these keys are bound within a restricted area, the intermediate nodes certainly get access to clear message text, which is not desired.

Simonova et al. (SLW) [16] suggested a localized deployment, where the entire network can be thought to be collection of subnetworks of nodes, each modeled with the design of [8]. Thus this scheme can be visualized as scaling a network built on the classic $TD(k, p)$ KPS [8]. However their amalgamation process enlarges the keyrings of the nodes of the final network. Alternatively, schemes such as [6] scale existing KPS like [8] without overburdening the keyrings of nodes of the ultimate network. Since all such schemes involve solution of higher order polynomial equations for growing networks, the scaling becomes restricted. Another problem faced by many existing KPS is the lack of full connectivity for the entire network. Such issues have been well addressed in the cluster based localized scheme [1]. A certain drawback of this scheme is the use of the special nodes (CH) with extra capabilities. These relatively expensive nodes increases the cost of the entire network, which may not be appropriate for certain applications.

Sarkar *et al.* [15] proposed the novel idea of distinguishing connectivity and communication of a sensor network while addressing the 'Selective Node Attack' and scalability issues, pertinent to most existing KPS such as [1,6–8,11,12,14–17]. Combination of the generic connectivity model of [15] with any KPS leads to highly secure networks. The UFD based KPS [14] provides a good example.

This KPS is fully connected and capable of supporting a large number of nodes even for small keyrings. One major drawback of this UFD based KPS [14] is its weak resiliency. This issue get appreciably addressed by the connectivity model of [15]. Since these schemes [14,15] uses relatively expensive special nodes with extra capabilities much like the KPS [1], networks designed on such schemes may not be appropriate for a specific application.

Extensive literature survey reveals all existing KPS, such as the ones analyzed in this work [1,6–8,11,12,14–17] and the references therein, try to strengthen the security of their protocol rather than exploiting the practical hazards faced by the adversary. The central idea of this work is to exploit the practical hazards faced by the adversary. One such hazard is the practical difficulties of tracing the frequency bands being used for inter–nodal communication, specially in adverse conditions. The focus then shift towards designing another level of security by assigning various frequency bands for distinct pairs of sensors in the same network. To the best of author's knowledge, this is perhaps the first proposal in WSN literature to propose a security model that exploits this practical weakness of tracing frequencies, encountered by the adversary.

The remaining part of this section is dedicated in reviewing some of the existing works related to Magneto optic sensors and their applications. Bera and Chakraborty [2] propose an experimental application that uses Magneto optic element as a displacement sensor. In this paper Terbium Doped Glass (TDG) has been taken for experimental purpose. A highly sensitive (with in 0.54 %) linear micro–displacement sensor with improved performance over an appreciable range of 10 mm and a resolution of 5 μm is achieved. The experimental data is in good agreement with the theoretical study.

Chakraborty and Bera [3] propose an experimental application of magneto optic element as an over-current detector. Over-current detectors (OCDs) are important components in system control but suffer from electromagnetic interference, noise, low response etc. But the potential advantages of using Magneto optic elements of immunity to ElectroMagnetic Interference (EMI), electrical isolation, large bandwidth, ease of integration into digital control system, potentially low cost.

Mahish and Chakraborty [9] proposed an experimental study of the characteristics of Magneto optic sensor using TDG as the magneto optic element. Experiments confirm that the general behavior of this sensor is non–linear. However under certain condition the sensor shows linear nature over a certain range about the operating points, which has been claimed theoretically. The authors suggests using this linear behavior for various applications. This linear behavior of the magneto optic TDG element has been exploited by the present authors while conducting the experiments.

2 Practical Hazard for Adversary: System Design and Analysis

The nodes are to be assigned with different frequency channels, unknown to the adversary. Assignment of different channels that are not known publicly ensures

their tracing by the use of 'Selective Filter(s)' becomes inconvenient and hence, expensive for the adversary. The entire network is to be assigned with a large number ($\mathbf{N}$) of frequency channels. The nodes are to be preloaded with a smaller number ($\mathbf{n}$) of frequency channels among the these $\mathbf{N}$ channels allocated for the entire network. This assignment is to be executed prior to the deployment of the network. For the sake of simplicity, $\mathbf{n}$ may be taken to be uniform (not mandatory) for all the nodes of the network.

Since the $\mathbf{n}$ frequency channels allocated to a node are not disclosed publicly, the adversary has to trace at least one of these $\mathbf{n}$ channels to get access to the transmitted information. Tracing all the $\mathbf{n}$ channels for any given node will naturally reveal all the information transmitted/received by it. Though the upper and the lower bound of the frequency range meant for the entire network may well be easily traceable by the use of an appropriate 'Selective Filter', tracking even one undisclosed band from a large ($\mathbf{N}$) set of frequency bands may be tough in adverse regions. This justifies the usefulness of the proposal of manufacturing nodes with several frequencies channels and allocating distinct pair of band(s) for distinct pair of nodes in the present case.

Further, since nodes can be deployed with different sets of $\mathbf{n}$ channels, the adversary has to use the 'Selective Filter' for individual nodes. Thus to nullify the additional security injected by the proposed method, the adversary has to figure out all the $\mathbf{n}$ channels of all the nodes. As the standard network size is in the order of thousands, this may be a rather expensive task for the adversary; if at all feasible.

Alternatively, assume a simpler case when the $\mathbf{N}$ bands meant for the entire network are somehow known to the adversary. However, the exact number of channels ($\mathbf{n}$) for each individual node is assumed to be still undisclosed. Further assume that no other information concerning the frequency bands is available to the adversary. This may compel the adversary to try and guess the allocated set of $\mathbf{n}$ bands for each node by reverting to the exhaustive search technique.

Tracking a single band for certain node may still be difficult task even after possessing the knowledge of all the $\mathbf{N}$ bands for the network. This is specially because there are thousands of nodes in the network lying in wide geographic area with varied degree of harshness. Tracing any band will involve tuning the 'Selective Filter(s)' to the exact band out of the $\mathbf{N}$ bands. This may be tough in adverse conditions. Clearly, the adversary's task of tracing all the $\mathbf{n}$ channels for a given node is not easy even on possessing the knowledge of all $\mathbf{N}$ bands of the entire network. This is because finding out all the $\mathbf{n}$ preallocated (unknown) bands for any given node among the $\mathbf{N}$ (known) bands for the network involve $\binom{\mathbf{N}}{\mathbf{n}} \approx (\mathbf{N}-\mathbf{n})^{\mathbf{n}}$ comparisons. Complexity of computation of any kind involving large numbers ($\approx 2^{80}$ bits) is high and is considered beyond the scope of modern day machine. The possibility of obtaining large value of $\mathbf{N}$ is assured by the wide range of Radio frequency (RF). A practical scenario is being described below.

Radio frequency (RF) range varies from around 3 kHz to 300 GHz. Each frequency channels of sensor networks may be allocated with a bandwidth of roughly 1 MHz (refer to [10]) to avoid interference (noise). So a practical choice

of $\mathbf{N}$ may be $\mathbf{3 * 10^5}$. For cost effectiveness, one may consider $\mathbf{n}$ to be $\mathbf{5}$. Thus a proposal of nodes having $\mathbf{5}$ bands amidst a total of $\mathbf{3 * 10^5}$ bands for the entire network is being made. Thus even in an unlikely case of knowing all $\mathbf{3 * 10^5}$ bands of the network, the adversary's task of tracing the exact $\mathbf{5}$ channels for each node is certainly difficult. This tracing of all the $\mathbf{5}$ preallocated (unknown) bands for any given node among the $\mathbf{3 * 10^5}$ (known) bands for the network involve $\binom{\mathbf{3*10^5}}{\mathbf{5}}$ comparisons, which is $\geq (\mathbf{2^{16}})^{\mathbf{5}} = \mathbf{2^{80}}$ comparisons. Such large comparisons is beyond the scope of all existing up-to-date computing devices.

3 Allocation of Frequency Bands: Frequency Graph v/s KPS Graph

Assuming the availability of low cost sensors with different sets of frequency bands, an application of this novel technology is being presented. The *target* is to make the sensors *transmit information automatically* through *various allocated channels* based on the *varying external vibrations* received by them. The parametric variations for an individual sensor may perhaps occur due to some external effect such as a sudden variation of the external impulse received by the node. The '$\mathbf{n}$' channels of each individual nodes can be paired with a maximum of n different sensors. This gives the flexibility of transmission of information to various nodes depending on *priority*.

For instance, during an emergency which may be indicated by a high external impulse, the sensors in harsh geographical conditions may choose to connect to nodes deployed at relatively safer positions. The phrase 'safer positions/locations' mean locations which are comparatively difficult for the adversary to access. Since the coverage area of any WSN is a large geographical area with varying degrees of harshness, such an argument is practical. This motivates the words 'safer nodes' which consequentially mean sensors falling within such 'safe positions/locations' and hence are less prone to physical capture. Since these 'safer nodes' are expected to be at a relatively distant position from the nodes placed at 'harsh locations', such communications may involve exchange of information through channels with high frequencies. Whereas for normal low external impulse, they may connect to nearby sensors via relatively low frequencies channels for analysis of the data before transmitting to distant 'safer nodes' for further processing. In case, any of the above communications are beyond the radio frequency range of the individual nodes, the encrypted information can be routed to the target entities via intermediate nodes. These 'safer' distant nodes can further analyze the aggregated data before ultimately routing the synchronized information to the BS.

The frequency bands can be *preallocated* in the nodes by the *system designer* to form a separate network graph, distinct from the existing graph of any KPS (key–graph). This separate graph shall be referred to as *frequency graph* of the network. This *frequency graph* imparts a natural *grouping* into the system. The scenario is similar to any *hierarchical* network barring the following key differences:

- Standard cluster based hierarchical network like [1,6,15,16] possessing specially designed nodes (CH) with extra capabilities result in an substantially increased cost of the overall network. These sort of designs generally have different network graphs for different levels of hierarchy.
- There exists odd designs like [16] amalgamates the keyrings of some existing KPS [8], thus burdening the memory of individual nodes of the existing network. This KPS has a inner cluster and a inter cluster graph.
- On the contrary, the current strategy provides a natural subdivision without any extra burden on the existing system. The proposed concept of use of different bands for pairing various node can be combined with an appropriate KPS. This combined resultant network possesses two separate graphs; (i) one owing to the existing KPS; and (ii) the other (*frequency graph*) emerging from the introducing of this novel concept of using separate frequency channels. The practicality of manufacturing sensors with desired small number (**n**) of distinct bandwidths have been justified above.

Thus one may achieve a secure KPS with a natural hierarchy without deploying special nodes with extra capabilities. This, according to the authors, is perhaps the first proposal of a truly distributed scheme achieving a natural hierarchy. This grouping can perhaps be exploited to design KPS with optimal security, i.e. security independent of the protocol design. This motivates the following analysis of the network deployment in order to allocate the various frequency channels for the individual sensors.

Random deployment of any wireless network implies that the nodes fall at varied distance from one another. This distance can be traced by the standard use of a Global Positioning System (GPS). The preallocated (by system designer) frequency channels for each nodes are to be paired with other nodes lying in their communication radius which may vary for individual bands. Since there are **n** channels per node, each of which forms a complete graph comprising of **n** vertex, i.e. nodes here. Thus the network is subdivided into segments of **n** complete graph for each of the **n** channels.

Having proposed partitioning of the network in terms of these varied undisclosed frequency channels, the focus now shifts to visualize a practical demonstration of the idea. Consider a practical example of network proposed for surveillance of enemy movement or another to monitor forest fire. Suppose, in the first case, a particular sensor senses heavy vibrations due to rapid infiltration. Such a case has to be reported immediately to the BS. Instead of analyzing with neighboring sensors, it may be worth to send the information directly to BS by routing via relatively 'safer' distant node(s). Similarly, in case of forest fire, suppose that drastic raise in temperature is noted by some sensor(s). Such an information must be passed onto the BS instantaneously. These real life instances demonstrates the applicability proposed concept.

Due the unavailability of sensors with different sets of multiple frequency bands meant for specific applications in WSN, real life experiments could not be performed. Instead, Magneto Optic sensors depend on Faraday's Magneto optic effect have been utilized to demonstrate the effect of a parametric change on the transmitted frequency.

4 Interplay Between Electromagnetic and Optical Medium

Performance of the Magneto Optic sensors depend on Faraday's Magneto optic effect, which was discovered in the year 1845. This effect says that when plane polarized light is sent through a Magneto Optic element in a direction parallel to the magnetic field, the plane of polarization gets rotated. Polarization of light is the vibration of the light wave in a particular plane. Natural unpolarized light wave vibrates randomly in any plane. So, at a particular time the vibrating plane of a particular wave cannot be determined. If this unpolarized light beam passes through a polarizer, then this permits vibration only in a particular plane. Then that particular wave is said to be a polarized beam for that particular plane. Thus, clearly the performance of these Magneto Optic sensors mainly depend upon the characteristics and properties of light, implying that their speed is as fast as light.

The association between Faraday's rotational angle (θ) related to *Electromagnetic waves* and the frequency of light (ϑ) corresponding to any *Magneto Optic* media is being highlighted in this section. When a linearly polarized light passes through a magneto-optic medium (e.g. a TDG), kept parallel to the magnetic field, the Faraday's rotation is given by the relation mentioned in Eq. 1.

$$\theta = V_{Verdet} B l \tag{1}$$

where V_{Verdet} is the Verdet constant and B is the *magnetic flux density* of the medium. l is the *length* of the *Magneto Optic element (TDG)*. The Verdet constant which is dependent on the wavelength of light can be expressed as:

$$V_{Verdet}(\lambda) = -\frac{e\lambda}{2mc}\left(\frac{dn}{d\lambda}\right) \tag{2}$$

Here, e denotes the *charge of an electron*, m is the *mass of an electron* while c is the *speed of light in vacuum*, which are always constants.

$$n(\lambda) = a + \frac{b}{\lambda^2} \text{ where, } a \text{ and } b \text{ are constants.} \tag{3}$$

n is the refractive index (RI) of the Magneto Optic medium, which depends on the wavelength (λ) of light as well as the Magneto Optic element. So,

$$\frac{\delta n}{\delta \lambda} = -\frac{2b}{\lambda^3} \tag{4}$$

For a particular Magneto Optic element (TDG, here), the refractive index is only function of λ. Thus Eq. 4 can be rewritten as:

$$\frac{dn}{d\lambda} = -\frac{2b}{\lambda^3} \tag{5}$$

Comparing $\frac{dn}{d\lambda}$ values from Eqs. 2 and 5, one concludes:

$$V_{Verdet}(\lambda) = -\frac{e\lambda}{2mc}\frac{2b}{\lambda^3} = -\frac{eb}{mc}.\frac{1}{\lambda^2} = \frac{K_1}{\lambda^2} \text{ where } K_1 = -\frac{eb}{mc}. \tag{6}$$

Again, it is well known that the relation between *wavelength* and *frequency* of any energy source is given by Eq. 7 below:

$$\lambda\vartheta = D(=c), c: \text{ meant for Optical medium}, \tag{7}$$

where D is the velocity of the energy source, which is constant for the given energy source. Since the work deals with Magneto Optics, hence conventionally, D is replaced by the symbol c. Thus in this paper, $D = c$. Combining Eqs. 6 and 7 yield the following Eq. 8.

$$V_{Verdet}(\vartheta) = \frac{K_1}{(c/\vartheta)^2} = \vartheta^2\frac{K_1}{c^2} = K_2\vartheta^2 \text{ where } K_2 = \frac{K_1}{c^2}. \tag{8}$$

So,

$$\theta(\vartheta) = K_2\vartheta^2 Bl \tag{9}$$

When the Faraday's rotation θ is 0° then the polarized optical beam vibrates at particular plane. This plane is called reference plane. Now with the change of θ, the plane of vibration also changes. So at particular rotation if the relative angle between the polarizer and analyzer remains constant then a component of the resultant optical beam will lie on the reference plane. This phenomenon can be expressed by the following equation, popularly known as Malus' law:

$$I = I_0 cos^2(\theta - \alpha) \tag{10}$$

where I_0 is the intensity of the optical beam when it vibrates at the reference plane. I is the component of I_0 which lies on a plane different of the reference plane. α is the relative angle between polarizer and analyzer. θ is the angle between the plane of vibration and the reference plane or in other way Faraday's rotational angle. Further, $I \propto V$, where V is the Photodiode voltage output, which can be approximated as a linear function of I. So, Eq. 10 yields:

$$V = V_0 cos^2(\theta - \alpha) \tag{11}$$

Combining Eqs. 9 and 11 yields:

$$V(\vartheta) = V_0 cos^2(K_2\vartheta^2 Bl - \alpha) \tag{12}$$

V is the voltage output when the optical beam vibrates at the reference plane. V_0 is the voltage output when the optical beam vibrates at the plane different from the reference plane.

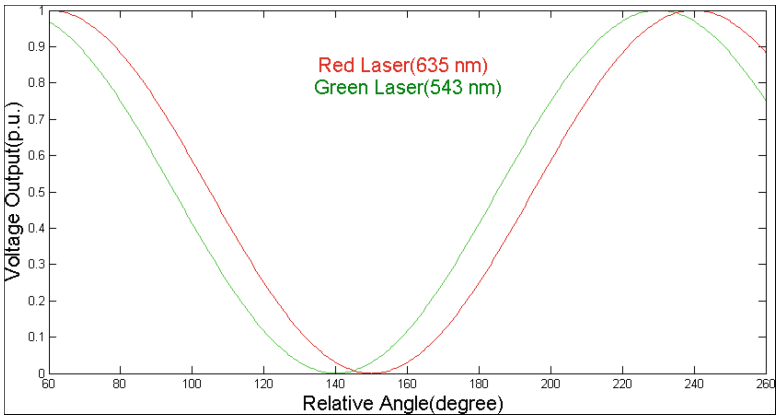

Fig. 1. Theoretical curve of voltage output with changing angle between polarizer-analyzer (Color figure online).

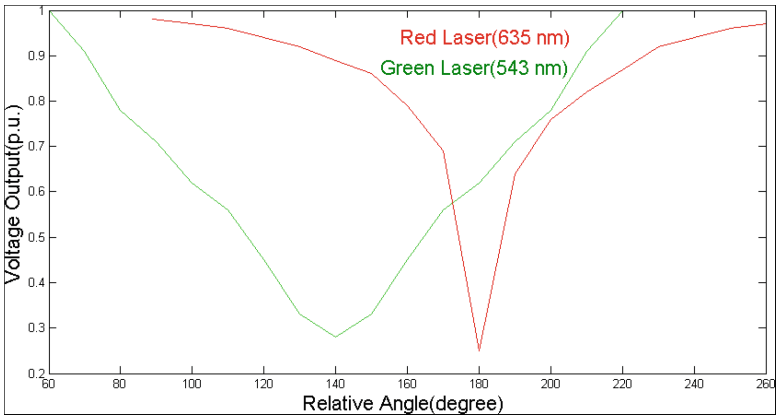

Fig. 2. Experimental curve of voltage output with changing angle between polarizer-analyzer (Color figure online).

5 Experiments and Results

Theoretical results based on Malus' equation have been sketched in Fig. 1. The theoretical figure shows the 10° constant relative difference between these two curves at a particular direction. This causes a 92 nm relative difference between red and green laser. However, the focus should be on the reduction of errors.

Due to limited facility, experiments could be conducted with only two different laser sources, red (635 nm) and green(543 nm). The results of the experiments have been presented in Fig. 2. The graphs in Fig. 2 expresses the change of Faraday's rotational angle with change in the wavelength of the optical wave. According to the change of relative angle between the polarizer and the ana-

lyzer, the component of the light intensity at reference plane will vary. This variation helps in tracing the individual curves. From the figure, it is clear that the position of the curve followed by red laser is shifted forward by approximately 40° than the curve followed by green laser at relative angle $60° - 180°$. This is caused by the relative difference of wavelengths between two different laser, i.e., $635 - 543 = 92$ nm. Thus it can be concluded that the experimental data resembles the theoretical data. Comparing these two distinct curves in Fig. 2, one may conclude that any change in wavelength of the laser causes variation in the Faraday's rotational angle at a particular direction. This may be generalized for other application specific sensors with corresponding parameters.

6 Conclusion

Unlike most existing works in the literature of WSN security which aims to strengthen their own protocol, this paper focuses on an weakness faced by the adversary; particularly in an adverse deployment zone. A practical hazard may be to trace the frequency channel used for communication between two sensors from a wide range of bands in a harsh geographical locations. Since the RF range is widely varied, use of 'Selective Filter(s)' to trace an unknown frequency may be an expensive affair; if at all feasible. This motivates the authors to think of allocating a large range (**N**) of frequency bands for the entire network. The low cost nodes are allocated with lesser no. (**n**) of frequency bands to ensure enhanced security. This concept of allocating various band to the nodes naturally partitions the entire network into groups. This is an added benefit since most existing schemes possessing an hierarchy utilized relatively expensive special nodes like cluster heads for such a subdivision. Unavailability of practically deployable application specific sensors meant that experiments were conducted with Magneto Optic sensors to prove the practicality of the claim that an external impulse may lead to parametric variations, and hence varied transmission of frequency for individual sensors.

7 Future Work

One promising future research direction steaming out of this work is the suggestion of manufacturing sensors with different sets of frequency channels. According to the authors' knowledge, such nodes are still not available commercially. In this connection, one is referred to a standard sensor configuration in [10] which is used universally for WSN applications. The practicality of the suggestion of manufacturing (numerous) nodes with different sets of multiple frequency channels has been set out in Sect. 1 while pointing out the availability of multi-Sim mobile phone handsets at a low cost.

A more challenging task may to construct low cost nodes capable of generating varied range of frequencies within individual sensors. Rohde and Schwarz [13] presents a vector signal generator which may pave a direction towards achieving this goal practically. This generator can act as an all in one test platform for

wireless devices. The generator supports cellular, non-cellular as well as broadcast technologies.

Once sensors capable of operating in multiple bands are availability, they may be used for practical implementation of the idea proposed in this paper. Based on an external impulse, transmission can made through desired band of the respective nodes. The varying transmission can be combined with some chosen existing and/or newly proposed KPS to ensure additional security for the encrypted message.

Acknowledgement. This work is partially done during Morshed Chowdhury's visit at Kouichi Sakurai's laboratory in Kyushu University-Ito Campus, Fukuoka, Japan, in June 2014.

References

1. Bag, S., Dhar, A., Sarkar, P.: 100% connectivity for location aware code based KPD in clustered WSN: merging blocks. In: Gollmann, D., Freiling, F.C. (eds.) ISC 2012. LNCS, vol. 7483, pp. 136–150. Springer, Heidelberg (2012)
2. Bera, S.C., Chakrabarty, S.: Study of magneto-optic element as a displacement sensor. Measurement **44**(9), 1747–1752 (2011)
3. Chakrabarty, S., Bera, S.C.: Magneto-optic over-current detection with null optical tuning. Sens. Transducers **87**(1), 52–62 (2008)
4. Çamtepe, S.A., Yener, B.: Combinatorial design of key distribution mechanisms for wireless sensor networks. In: Samarati, P., Ryan, P.Y.A., Gollmann, D., Molva, R. (eds.) ESORICS 2004. LNCS, vol. 3193, pp. 293–308. Springer, Heidelberg (2004)
5. Çamtepe, S.A., Yener, B.: Key distribution mechanisms for wireless sensor networks: a survey. Technical report, Rensselaer Polytechnic Institute, Rensselaer Polytechnic Institute, Lally 310110, 8th Street, Troy, NY 12180–3590 (2005). http://www.cs.rpi.edu/research/pdf/05-07.pdf. Last Accessed: July 14, 2014
6. Chakrabarti, D., Seberry, J.: Combinatorial structures for design of wireless sensor networks. In: Zhou, J., Yung, M., Bao, F. (eds.) ACNS 2006. LNCS, vol. 3989, pp. 365–374. Springer, Heidelberg (2006)
7. Lee, J.-Y., Stinson, D.R.: Deterministic key predistribution schemes for distributed sensor networks. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 294–307. Springer, Heidelberg (2004)
8. Lee, J., Stinson, D.R.: A combinatorial approach to key predistribution for distributed sensor networks. In: WCNC, pp. 1200–1205 (2005)
9. Mahish, P., Chakrabarty, S.: Study of magneto optic sensor using TDG element. Int. J. Innovative Res. Electr. Electron. Instrum. Control Eng. (IJIREEICE) **1**(6), 254–258 (2013)
10. Moteiv Corporation. Tmote sky: Datasheet (2006). http://www.eecs.harvard.edu/konrad/projects/shimmer/references/tmote-sky-datasheet.pdf, Last Accessed: July 14, 2014
11. Paterson, M.B., Stinson, D.R.: A unified approach to combinatorial key predistribution schemes for sensor networks. Des. Codes Cryptography **71**(3), 433–457 (2014)
12. Ren, K., Lou, W., Zhang, Y.: LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks. IEEE Trans. Mob. Comput. **7**(5), 585–598 (2008)

13. Rohde and Schwarz. R&S® CMW500 Wideband Radio Communication Tester (2009). http://d3fdwrtpsinh7j.cloudfront.net/Docs/datasheet/rs_cmw500_overview.pdf, Last Accessed: July 14, 2014
14. Sarkar, P., Chowdhury, M.U.: Key predistribution scheme using finite fields and reed muller codes. In: Lee, R. (ed.) Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing 2011. SCI, vol. 368, pp. 67–79. Springer, Heidelberg (2011)
15. Sarkar, P., Saha, A., Chowdhury, M.U.: Secure connectivity model in wireless sensor networks (WSN) using first order Reed-Muller codes. In: MASS, pp. 507–512 (2010)
16. Simonova, K., Ling, A.C.H., Wang, X.S.: Location-aware key predistribution scheme for wide area wireless sensor networks. In: SASN, pp. 157–168 (2006)
17. Wei, R., Wu, J.: Product construction of key distribution schemes for sensor networks. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 280–293. Springer, Heidelberg (2004)