ISSN 2047-3338

A Survey about Security of the Wireless Sensor Network

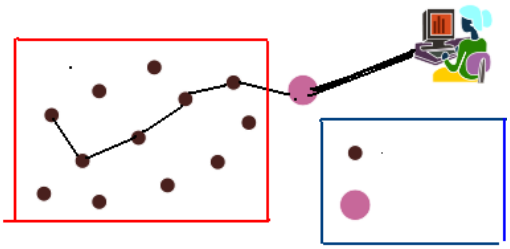
Irfanullah Khan, Faheem Khan, Lala Rukh, Zaidullah and Yasir Ali
Gandahara University Peshawar, Pakistan
Agriculture University KPK Peshawar, Pakistan

***Abstract*– The considerable advancement of Hardware manufacturing Technology and the progress of Efficient Software Algorithms formulate technically and economically feasible a Network consist of a range of, small, low-priced Sensors by means of Wireless Communications, that is, a Wireless Sensor Network. Wireless Sensor Network has fascinated thorough importance from both academic world and Industry as of its broad Application in civil and military situations. In intimidating situations, it is very vital to defend Wireless Sensor Network from malevolent Attacks. As of a range of resource limitations and the salient features of a Wireless Sensor Network, the Security plan for Such Networks is considerably demanding. In this Article, we offer complete Survey of Wireless Sensor Network Security matters, which were inspected by Researchers in present years and that shed light on future direction for Wireless Sensor Network Security.**

***Index Terms*– WSN, Security, Challenges and Features**

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of spatially disseminated autonomous Sensors to check physical or environmental environments, like temperature, sound, vibration, pressure, motion and humidity and to transmit their information through the network to the main Location cooperatively [1]. The further up to date Networks are bi-directional, as well enable control of Sensor movement. The progress of Wireless Sensor Networks was provoked by military Applications for Example battlefield observation; nowadays Such Networks are executed in many industrial and end User Applications, like industrial procedure observe and control, machine health supervising, etc. The Wireless Sensor Network is build of "Nodes" – from a



· Sensor Node
· Gateway sensor node

Fig. 1. Typical multi-hop wireless sensor network architecture

few to Several Hundreds or even Thousands, where every Node is linked to one (or sometimes Several) Sensors. Each and every Such Sensor Network Node has normally Several parts: a Radio transceiver having an Internal Antenna or link to an External Antenna, a micro controller, an electronic circuit for crossing point by means of the Sensors and an Energy resource, Typically a battery or an embedded form of Energy production. A Sensor Node may differ in volume from the shoebox to the size of the grain of the dust, even though working "motes" of authentic microscopic proportions have up till now to be produced. The price of Sensor Nodes is likewise changeable; depend on the complication of the individual Sensor Nodes. Size and price restrictions on Sensor Nodes effect in resultant restrictions on assets like energy, memory, and computational rapidity and communications bandwidth. The topology of the Wireless Sensor Network can be able to differ from a Simple star Network to a sophisticated multi-hop wireless mesh network. The Propagation technique among the hops of the Network knows how to be routing or flooding [2], [3]. In computer science and telecommunications, Wireless Sensor Networks are an energetic Research spot by means of a variety of workshop and conferences approved every year. The considerable advancement of Hardware industrialized Technology and Efficient Software Algorithms formulate a Network consist of a range of, undersized, low-priced Sensors, by technique of Wireless Communication. A Wireless Sensor Network (WSN) [1]–[3] is a capable Network Infrastructure for numerous Applications Like environmental observe, medical concern, and domestic device managing. This is mainly proper for battlefield observation and homeland safety situations as Wireless Sensor Network are simple to organize for those Applications. Nevertheless, in numerous threatening and planned situations and vital business Applications, Security means are necessary to defend Wireless Sensor Network from malevolent hits. So, the safety measures in Wireless Sensor Network turn out to be an vital and demanding plan charge.

II. SECURITY CHALLENGES

Wireless Sensor Network has much distinctiveness that completed them very susceptible to malevolent Attacks in intimidating Environments like military battleground:

• A wireless medium is technique able to everyone. By means of a radio interface configured at the same frequency band, anybody can observe or contribute in communications. This offers an easy technique for attackers to indulge into wireless sensor network.

• As in the Internet, the greater parts of protocols for wireless sensor network do not include potential security considerations at the plan stage. As of standard activity, the greater part of protocols is identified widely. As a result, attackers by means of out complexity start attacks by exploit security holes in those protocols.

• The limited resources make it very complex to execute strong security algorithms on a sensor stand as of the complexity of the algorithms on the other hand, fragile security protocols be capable to be broken down easily by attackers.

• A wireless sensor network is typically installed in intimidating vicinity by means of any permanent infrastructure. It is complex to execute constant observation after network deployment. As a result, a Wireless Sensor Network may face diverse attacks.

III. SECURITY REQUIREMENTS

The severe environments and the presence of threats demand more cautious security concerns in the plan of Wireless Sensor Networks Protocols. Typically, one or more of the following security services must be offered:

• *Confidentiality* is a fundamental security service to preserve the privacy of vital information transmitted among sensor nodes.

• *Authenticity is* important to offer the guarantee of the distinctiveness of communicating nodes.

• *Integrity* must be offered to guarantee that attackers do not customize the pass on messages.

• *Availability* shows another vital ability of a Wireless Sensor Network to offer services when they are necessary.

A. The Organization of this Article

The most important character of Wireless Sensor Network and the continuation of a variety of malevolent attacks pose considerable confronts to the plan and deployment of security protocols for Wireless Sensor Network. Though some surveys [4]–[8] explain in general the confronts of and rationales for planning security protocols for Wireless Sensor Network, they either do not clearly organize or discover the Security issues that the greater part of researchers are still examining or they spotlight frequently on definite precise topics. Furthermore, these papers do not cover up the most recent progress in this vicinity, although security-important applications of Wireless Sensor Network have motivated several issues linking to security plan for Wireless Sensor Network in the last few years. In this paper, we offer a survey of security issues and the most recent explanations for wireless sensor network, and we discover related open issues for future research. Key organization is the first step to ascertain a security infrastructure as all encryption and a*uthentication* procedures must engage keys. We talk about present key establishment designs. Authentication, as well as i*ntegrity* security, is also talk about. On availability we are having two topics. Routing is important to offer information delivery services. We talk about the detection of malevolent attacks that can damage network functionality. Usual applications of Wireless Sensor Network are discussed, and then the article is concluded.

IV. KEY ACHIEVEMENT

The greater part of security protocols is based on cryptographic procedures that engage keys. To offer confidentiality, an encryption procedure necessitates a key to be fed into an algorithm so that the plaintexts can be altered into Cipher texts. To guarantee packet authenticity, the source node can connect a MAC to each and every packet, where typically, the MAC is computed by hashing the concatenation of the packet and a key. Two kinds of keys are used in cryptographic systems. The first one is the *symmetric key*, of which Claude Shannon established the theoretical framework in his classic paper "Communication Theory of Secrecy Systems" [9].

In a symmetric key system, the sender and the receiver share a general key that is kept undisclosed from others. The sender encrypts a plaintext *M b*y means of the key K by an Encryption algorithm E to get a Ciphertext $C = E(M, K)$. After receiving the Ciphertext *C*, the Receiver inputs *C* and the Key *K* into a Encryption Algorithm *D* To get the orignal Plaintext $M = D(C, K)$. The next widely used type is the *Asymmetric Key*, that was first studied in [10], [11]. In an Asymmetric Key System, each and every User has a Pair of Keys $\{Ks, K p\}$. The User keeps undisclosed his *Private Key*, *Ks*, at the same time as publishing his/her *Public Key*, *Kp* When a Sender wants to Send a Plaintext *M* to a Receiver, the Sender uses the Receiver's Public Key, *Kp*, to Encrypt *M* to get a Ciphertext $C = E(M, Kp)$.

Only the Receiver can use his Private Key to Decrypt the Ciphertext and get $M = D(C, Ks)$ as only the Receiver knows his own private key, *Ks*.

As a public key is used here, typically asymmetric key systems are called public key systems. The security of a cryptographic system depends mostly on the privacy of the key it uses. If an attacker can discover the key, the complete system is broken as the attacker can use the key to decrypt the Ciphertexts to discover the orignal plaintexts. The attacker can attain the objective by cryptanalysis on the Eavesdropped packets that are sended out over the wireless medium. As of the presence of the redundancy of the message source in the real world, the attacker may know more or less information about the key used. As a result, the sender and receiver may be necessary to bring up to date the key used among them from time to time.

In a Wireless Sensor Network, an attacker may capture some sensor nodes. As a result, a very vital issue is how to protect control the keys between the sender and the receiver. Keys also can be organized into two groups according to dissimilar communication patterns in Wireless Sensor Network. One is the *Unicast Key* among pair of nodes. A pair wise general key must be established to protect the unicast communication. The other is the b*roadcast/multicast key* among a group of nodes. A group key is necessary to protect the cluster communication.

In general, to establish keys in a Wireless Sensor Network includes two steps. Before sensor nodes are deployed, each and every node is configured by means of some key materials. After those nodes are deployed into a designated terrain, they perform several rounds of communications to agree on the keys computed by means of their key materials. Based on the algorithms used to ascertain pair wise keys, present explanations can be classified into symmetric key designs and asymmetric key (or public key) designs. In this section, we talk about pair wise key designs, including symmetric and asymmetric ones; then, group key achievement; and last, open issues.

V. SYMMETRICKEY ACHIEVEMENT

The greater part of symmetric key algorithms, like information encryption standards (DES) [12] or Rivest Cipher 5 (RC5) [13], need simple Hash, rotation or scrambling procedures that can be efficiently executed in hardware or software. As the symmetric key technology is more practical on resource controlled low-end devices than the asymmetric key technology. Most of the security protocols in the survey for Wireless Sensor Network are depend on symmetric key technology. A fundamental issue for applying the symmetric key technology is how to start a symmetric key between two sensor nodes. A straightforward technique is to allocate a *Global Key* [14] to all the sensor nodes. This technique is protecting from external attackers as the key can be exposed if a node is cooperated.

Due of the presence of BSs, centralized key allocation [15] can be used. In particular, each and every Sensor Node distributes a distinctive key by means of a BS, which acts as a key allocation center (KDC). If two nodes must correspond protect, they can attain a general key from the BS, which unicasts the key to each and every of them. This centralized technique could acquire a large amount of communication overhead as two adjacent nodes might be necessary to do handshakes from a central key server at distant place.

The greater part of current explanations to key establishment in Wireless Sensor Network pursue a allocated technique, called k*ey pre-allocation*, where every sensor node is preloaded by means of the key materials by means of which to establish general keys by means of other nodes after being deployed into the network terrain. There are two components in this technique: one is how to establish a general key by means of key materials, and the other is how to allocate key materials. In the plan of the allocated technique, several issues must be measured:

A. Random Key Material Distribution

The key agreement models explained can guarantee that every pair of nodes in a network of *N n*odes has a unique general key, but the cost is that all the nodes must store $N - 1$ keys. This is unreasonable for Wireless Sensor Network due to the memory restrictions of sensor nodes and the probable great range of sensor networks. As an alternative, the greater parts of existing research papers in this field settle down the security constraint and pursue a *partial* pre-allocation technique, where key materials are pre-allocated such that some sensor nodes can establish general keys directly and then facilitate to establish indirect general keys among other sensor nodes. A usual plan is the random key pre-allocation (RKP) [16] a main concern of RKP is Node negotiation.

To lessen the impact of node negotiation, the following designs are planned: *q-Composite RKP* [17] pursues RKP excluding that a pair of adjoining nodes is necessary to share at least *q* keys by means of a definite probability; *q-Composite* RKP can progress the elasticity to node compromise when the number of compromised nodes is little. Unluckily, it is not efficient when the number is huge. Spatial diversity is exercised in [18] to progress the elasticity to node compromise. Mainly, there are some influential anchor nodes that are suppose d to be interfere proof. A global key is general by all the anchor nodes and normal nodes, and each and every normal node is preloaded by means of a key ring following RKP. Each and every anchor node exercises the global key to broadcast several rounds of random nonces at dissimilar power levels in its vicinity.

Each and every sensor node uses the received nonces to restore its key ring. Later, all the nodes can pursue RKP to establish general keys by means of their neighbors. In conclusion, each and every node erases its original key ring and the global key. The initiated spatial diversity by anchor nodes results in the derived key rings being very dissimilar for two nodes that are far a technique from each and every other, while making adjoining nodes have more general keys in their derived key rings. As a result, the impact of node compromise is incomplete in the local vicinity. On the other hand, these techniques suppose that the new Nodes can maintain node compromise in its initialization phase. Furthermore, the introduction of anchor nodes increases the price of deploying a Wireless Sensor Network.

B. Location-Based Key Materials Allocation

In the aforementioned random and Deterministic Key materials allocation designs, Key materials are regularly allocated in the whole terrain of a Network. The uniform allocation formulates the probability relatively small that two adjoining Nodes share a direct Key at one hop, that is, local protect connection. As a result, a lot of Communication Overhead is expected for the Establishment of indirect Keys over multihop paths. To progress the local protect connection, many Researchers suggest to engage location information in Key Establishment [19–23]. In the Location-based Key pre-allocation (LBKP) techniques [19], the entire Sensor Network is divided into square cells. Each and every cell is connected by means of a Unique t-degree bivariate Polynomial. There are other designs that simply change the Polynomial model by means of other RKP designs Such as RKP [16] in [20] and MSKP [24] and RPK [17] in [21].

C. Comparison of Symmetric Key Design

Here, we estimate random [16], [17], deterministic and location-based [19]–[23] designs. First, in Table 1, we evaluate the memory costs of dissimilar designs. Random allocation designs require that each and every node stores a key ring. To preserve a certain level of connection, the size of a key ring cannot be undersized and typically at the level of O

(*N*). . Graph-based deterministic allocation designs [25]–[18] also need that each and every node stores a key ring. The memory cost of these designs is either O (*N*) for usual graph or O (♪*N)* for BIBD plan. Grid-based deterministic designs [18] have the memory charge only at the level of O (♪*N) Where k* > 1, as they use a *k*-dimension grid to categorize the Network. The greater part of Location-based designs [19]–[23], [32]–[33] combine location information and random allocation designs and have less memory cost than random allocation designs. Their memory cost is:

Table 1: Memory cost (N) is the total number of nodes in the network; (k) is the number of dimensions

Key material distribution approach	Schemes	Memory Cost
Random	[16, 17]	O (*N*)
Deterministic	Graph based [25–18]	O (*N*) or □. ♪*N*
	Grid based [37]	□. ♪*N*
Location-based	[19–23] [32–33]	O (*N*) or □. ♪*N*
	[30-31]	□. ♪*N*

O (*N*) or O (♪*N*). One exception Is [30-31], where Location Information and the Deterministic Techniques [18] are combined, and thus the Memory cost of [30-31] is □. ♪*N*.

Next we evaluate the Resilience to Node Compromise in Table 2. Typically, the probability of link Compromise can be used to evaluate the Resilience to Node Compromise as The Key Information in Compromised Nodes can be used to derive the Keys used by the links among non-Compromised Nodes. For the designs [16], [17], in which Keys are directly pre-allocated, the link Compromise probability Is approximately linear by means of respect To The number of Compromised Nodes as every time one More Node is Compromised, more Keys from the Global Key Pool is disclosed. On the other hand, matrices or Polynomial-based Designs have a useful property of Threshold-based Resilience, which means the Network, can endure Up to a definite number of Compromised Nodes while still Keeping the links among non-Compromised Nodes safe.

Table 2: Resilience to Compromise Node

Key agreement model	Schemes	Link Compromise Probability
Predistributed keys	[16, 17–18, 33]	App linear or quickly increasing to number of Compromised Nodes
Matrices or polynomials	[24, 31, 29, 32]	Threshold- based

Table 3 shows the local protect of dissimilar designs. The local protect connection of uniform allocation designs [16], [17] is lower than that of location-based designs [19]–[23]. As a result, by combining location information, Each and every node can establish direct keys by means of additional nodes and there by save energy on the establishment of indirect keys all the way through multichip routs by means of other neighbors. Last, in Table 4 we summarize the difference among the aforementioned key pre-allocation designs [16], [17] and other special designs [34]–[35]. The main divergence is the security assumptions. The greater part of talk about technique in the literature [16], [17] suppose strong Attackers by means of powerful abilities in terms of unlimited time and spatial cover up age, But a fragile attack model also is studied in [34]–[35].

Table 3: Local security connectivity

Key material deployment pattern	Schemes	Local security connectivity
Uniform	[16, 17–18]	Low
Location-based	[43–54]	High

Table 4: Comparisons with other schemes

Schemes	Security assumption	Memory Cost	connectivity
[16, 17–34]	Strong attackers with strong capibilities	Large	Low for uniform Key material deployment and high for Location-based Key material deployment
[34-35]	Weak attackers with limited capibilities	Small	High

The dissimilar plans result in dissimilar memory cost and connection performance, where the trade-off among security and performance can be marked. Designs [16], [17] require a large memory cost to tolerate node compromise and offer acceptable connection, while designs [34]–[35] have a smaller memory cost and elevated connection by means of feeble resilience to node compromise.

VI. ASYMMETRICKEY MANAGMENT

Though it is very computationally costly, asymmetric key technology is easier to achieve and more resistant to node compromise than symmetric key technology. Each and every node can keep undisclosed its private key and only issue its public key; As a result, compromised nodes cannot offer clues to the private keys of non-compromised nodes.

Computational Efficiency: In recent times, some researchers initiated to examine the possibility of use of asymmetric key technology on sensor platforms as of the fast progress in hardware capability. The greater part of challenging issue here is how to perform asymmetric key algorithms in an efficient technique. One technique is to use definite limitations that can speed asymmetric key algorithms by means of out compromising security. For example, Tiny Public Key (Tintype) [36] uses RSA-based certificates to authenticate external parties before they can entrance the

network, where the RSA [18] public key is selected, as $e = 3$, such that the signature validation at the sensor side is simplified. Furthermore, the Daffier-Hellman Algorithm [17] is used in Tintype [36] to exchange keys among sensor nodes, where the base of exponentiation is selected as 2, Such that the exponential procedure is easy. Another technique is to use customized hardware plan to simplify asymmetric key procedure. Gambits, Kips, and Sonar [64] showed the achievability of executing the Rabin techniques [38] and the Ntru Encrypt techniques [39] on a customized hardware platform.

Applications: In addition to RSA for Authentication and Diffie-Hellman for key establishment [36], ECC also is interesting importance for the security plan of wireless Sensor network as of its efficiency. Huang *et al.* [40] measured a Sensor Network consisting of protect achievers and several sensor nodes. An ECC based authenticated key establishment protocol is proposed for the key establishment among protect achievers and sensor nodes. To reduce the computational overhead of sensor nodes, the greater part of computationally costly asymmetric key operations are put on the protect achiever side. In precise, the Elliptic Curve Digital Signature Algorithm (ECDSA) [41] is used to authenticate new sensor nodes when they join the network, and the ECC based Diffie-Hellman Algorithm is used to establish common keys among sensor nodes.

Authenticate Public Keys: Another important issue of relating Asymmetric key technology is the authenticity of public keys. The node must keep a public key those assertions to have it. Then, attackers can easily impersonate any node by claiming its public key and start the *man-in-the-middle* attack. However, technical progression unites the use of asymmetric key technology feasible in wireless sensor network; asymmetric key algorithms are further costly than symmetric key algorithms. The authentication of public keys still may suffer high energy utilization, as authentication is possible to be achieved many times. In the merkle tree, each and every parent is a Hash of the concatenation of its children, and each and every leaf resembles to a node and is calculated as a Hash of the node ID and its public key.

Open Issues: The greater part of present symmetric key designs for Wireless Sensor Network aim at *link layer security* for one-hop communications, but not the *transport layer security* for multihop communications, as typically, it is not likely for each and every node to store a transport layer key for each and every of the other nodes in a network as of the huge number of nodes. Asymmetric key technology is costly but has flexible achievability. Any pair of nodes can establish a general key by means of asymmetric key techniques. A more promising technique is to combine both techniques, such that each and every node is prepared by means of an asymmetric key system and depends on it to establish end-to-end symmetric keys by means of other nodes. To achieve this objective, an important issue is to develop more efficient asymmetric key algorithms. How to prove the authenticity of public keys is another vital issue. Identity-based cryptography is a shortcut to stay away from the issue. There still is a requirement for the progress of more efficient symmetric key algorithms as encryption and authentication based on symmetric keys are very normal in the security procedures of sensor nodes. When a node is identified as a malevolent one or as a compromised one, its key must be revoked such that it cannot contribute in normal communications. As there are so many designs following dissimilar techniques, it is very complex to plan universal key revocation techniques. It is still an open issue for resource controlled wireless sensor network.

Protect Routing: The objective of networking is to offer an infrastructure for delivering information from a source node to a destination node. Routing protocols are the greater part of important component as they address the issue of how to find a path from the source to the destination and finally take charge of information delivery. In this technique, the nodes in a network can collaborate by means of each and every other to fulfill a range of applications deployed in advance. If routing protocols fail under malevolent attacks, the high layer applications also fail and the network is useless. As a result, protect routing is very vital to guarantee the network functionality in the face of malevolent attacks.

Issues: To reduce energy utilization, routing techniques for Wireless Sensor Network utilize well-identified tactics, as well as those exacting to Wireless Sensor Network [42]. For example, in flat routing protocols such as directed diffusion [43], information aggregation and in network processing are necessary to lessen the number of transmissions of redundant information. Clustering is a important procedure to build up a hierarchical Wireless Sensor Networks in hierarchical routing protocols like the low energy adaptive clustering hierarchy [44]. Sensor nodes in the local vicinity assist to select a cluster head that might be further influential so that it can perform more composite procedures like information aggregation or long distance routing. In location-based routing protocols like geographical and energy-aware routing (GEAR) [45], the location of a sensor node, which can be predictable by global positioning system (GPS) devices or GPS-free techniques, is used as the routing metric.

On the other hand, the greater part of routing protocols [42] for Wireless Sensor Network does not consider security in their plans. Karlof and Wagner [6] pointed out that the greater part of routing protocols for Wireless Sensor Network is susceptible to malevolent attacks. Unencrypted packets that carry routing information can be simply subject to eavesdroppers so that attackers can discover up the network topology. Attackers can insert fake routing information to start a Sybil Attack [46], [47] or redirect Packets to change network topology [48], [49]. Both of the attacks can change the network traffic prototype so that some malevolent nodes can receive most of the traffic before it appears at the BS.

In information aggregation, the aggregation node can be compromised so that the aggregated information is interfered by means of a non-aggregation node also can report fake information to the aggregation node to disturb the final report. A location deterministic procedure is susceptible as it necessitates co procedure among several nodes and may not be flourishing if some of them are malevolent. A malevolent node purposely may drop some of the passing traffic. Selective forwarding is more complex to detect. A malevolent node may fall the packets from some selected nodes and

forward those from other nodes. A subtler technique is to fall packets irregularly so that it behaves like an unbalanced medium. The greater part of routing protocols requires that each and every sensor node periodically broadcast routing information to preserve the network topology. If the time synchronization in the preservation procedure is attacked the entire network fails. Though several suggestions tried to protect ad-hoc routing protocols, they barely can be functional in wireless sensor network for three bases. First, those proposals all aim ad-hoc networks, which are dissimilar from Wireless Sensor Network in terms of resources and communication models [50]. Second, those proposals are security extensions of presented ad-hoc routing protocols like dynamic source routing (DSR), (AODV), or (DSDV), which are not appropriate for Wireless Sensor Network.

Third, those proposals need either asymmetric key cryptography or complex symmetric key cryptography, which are costly on Sensor platforms.

Available Explanations: Several promising security countermeasures for secure routing protocols are talked about in [50]. Link-layer encryption and authentication by means of a global key can defend Wireless Sensor Network against external attackers, as they do not know the global key. On the other hand, this does not protect against node compromise as the global key can be exposed. A trustful BS can detect spoofed node identities if every node shares a unique key by means of it, which is studied in SPINS [51]. On the other hand, the centralized control can introduce too much communication or achievement overhead. To support topology maintenance, authentication is necessary to defend broadcast of routing information in local vicinity. Though these techniques efficiently can avoid external attackers from spoofing, modify, and replaying information and lessen the impact of selective forwarding, they cannot defend the network from internal malevolent nodes efficiently.

In the intrusion-tolerant routing protocol for Wireless Sensor Networks (INSENS) the BS can collect the authentic routing information so that it can calculate the routing table for every sensor node. The broadcast information from the BS is authentic by a one-technique Hash chain. To prevent DoS attacks, individual nodes are not allowed to broadcast information to the entire network. To increase the patience to node compromise, redundant multipath routing is used so that traffic can endure even if some routs are compromised.

On the other hand, INSENS suppose an application situation where communications can occur only among sensor nodes and the BS. It does not sustain in network processing. Pietro *et al.* planned an expansion of logical key hierarchy for wireless sensor networks (LKHW) to defend the directed diffusion protocol [43]. An LKH is a key tree structure by means of source nodes as leafs and sink nodes as the root. Each and every leaf node holds keys along the path from it to the root node. In LKHW, an LKH is established before information is fused. Then the LKH is used to offer encryption and Authentication for information fusion.

VII. INTELLECTUAL PROPERTY SECURITY

When information sensing and processing turn out to be the main application of a Wireless Sensor Networks the intellectual property intellectual property is of vital significance to avoid the duplication of the sensed or processed information. As a result, there is an insistent obligation to enlarge intellectual property security (IPP) Techniques. The several watermarking techniques were developed to embed cryptographically encoded authorship signatures into information and information attained by Wireless Sensor Network. The key inspiration is to compel additional restraints throughout the information acquisition or sensor information processing. One technique is to watermark raw information through the sensing procedures by modifying the location and orientation of a sensor, time accomplishment discipline (e.g., Frequency and phase of periods among successive information capturing), and its explanations. The second technique implants a signature during information processing, in which some differences are introduced into information processing measures like error minimization procedures, physical world model building, and resolving of computationally inflexible issues.

Open Issues: Though Wireless Sensor Network have been establish to be helpful in a wide variety of applications, researchers and engineers are still appearing for new and capable applications that can increase the development of the whole vicinity and motivate a beneficial market. Dissimilar applications may have dissimilar Security necessities, which may be reliant on precise security plans. Cautious security plan at low layers as well as encryption and authentication may not efficiently avoid attacks at the application layer as they cannot understand and the semantics at the application layer. Oppositions can increase any information that can be demonstrated only by applications. As a result, it is essential to include security resilience into the application layer before we organize a new Wireless Sensor Networks Application.

VIII. CONCLUSION

Security is becoming a main apprehension for Wireless Sensor Networks Protocol planers as of the wide security-important applications of Wireless Sensor Network. In this paper, we talked about general security issues in Wireless Sensor Network and explained consequent explanations. On the other hand, there are still many open issues. On the one hand, Wireless Sensor Network is still under improvement, and many protocols planed so far for Wireless Sensor Network have not taken Security into concerns. On the other hand, the significant features of Wireless Sensor Network generate it very challenging to plan strong security protocols while still conserving low Overheads. Therefore, wireless security for Wireless Sensor Network is still very productive Research vicinity to be discovered.

REFRENCES

[1] Clare, Loren P., Gregory J. Pottie, and Jonathan Agre (1999). "Self-Organizing Distributed Sensor Networks." Proc. SPIE Aero-sense 99.

[2] Dargie, W. and Poellabauer, C., "Fundamentals of wireless sensor networks: theory and practice", John Wiley and Sons, 2010, pp. 168–183, 191–192

[3] Sohraby, K., Minoli, D., Znati, T. "Wireless sensor networks: technology, protocols, and applications, John Wiley and Sons", 2007, pp. 203–209

[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," Commun. ACM, vol. 47, no. 6, June 2004, pp. 53–57.

[5] E. Shi and A. Perrig, "Designing Secure Sensor Networks," IEEE Wireless Commun. Mag., vol. 11, no. 6, Dec 2004, pp. 38–43.

[6] F. Hu and N. K. Sharma, "Security Considerations in Ad Hoc Sensor Networks," Elsevier Ad Hoc Networks, vol. 3, no. 1, 2005, pp. 69–89.

[7] J. P. Walters and Z. Liang, "Wireless Sensor Network Security: A Survey," Security in Distributed, Grid, and Pervasive Computing, Ed. Y. Xiao, Auerbach Publications, CRC Press, 2006.

[8] S. Avancha et al., "Security for Wireless Sensor Networks: Overview," Wireless Sensor Networks, Ed. C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Kluwer Academic Publishers, 2004.

[9] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell Sys. Tech. J., vol. 28, Oct. 1949, pp. 656–715.

[10] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. Info. Theory, vol. IT-22, no. 6, 1976, pp. 644–54.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public key Cryptosystems," Commun. ACM, vol. 21, no. 2, Feb. 1978, pp. 120–26.

[12] FIPS PUB 46-2, "Data Encryption Standard (DES)," Dec. 1993.

[13] IETF RFC 2040, "The rc5, rc5-cbc, rc5-cbc-pad, and rc5-cts algorithms," Oct. 1996.

[14] S. Basagni et al., "Secure Pebblenets," Proc. 2nd ACM Int'l. Symp. Mobile Ad Hoc Networking and Computing (Mobihoc'01), Long Beach, CA, 2001.

[15] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," ACM Wireless Networks, vol. 8, no. 5, Sept. 2002, pp. 331–34.

[16] L. Eschenauer and V. Gligor, "A Key Management Scheme for Distributed Sensor Networks," Proc. 9th ACM Conf. Computer and Communications Security (CCS'02), Washington, DC, Nov.2002.

[17] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. 2003 IEEE Symp. Security and Privacy, May 2003, pp. 197–213.

[18] F. Anjum, "Location Dependent Key Management Using Random Key-Predistribution in Sensor Networks," Proc. 5th ACM Wksp Wireless Security (WiSe'06), Los Angeles, Sept. 2006.

[19] D. Liu and P. Ning, "Location-Based Pairwise Key Establishments for Relatively Static Sensor Networks," Proc. 2003 ACM Wksp. Security of Ad Hoc and Sensor Networks (SASN'03), Fairfax, VA, Oct. 2003.

[20] W. Du et al., "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," Proc.23rd Annual IEEE Joint Conf. IEEE Computer and Communications Societies (INFOCOM'04), Hong Kong, Mar. 2004.

[21] D. Huang et al., "Location-Aware Key Management Scheme for Wireless Sensor Networks," Proc. 2nd ACM Wksp. Security of Ad Hoc and Sensor Networks (SASN'04), Washington, DC, Oct. 2004.

[22] Z. Yu and Y. Guan, "A Robust Group-Based Key Management Scheme for Wireless Sensor Networks," Proc. 2005 IEEE Wireless Commun. and Networking Conf. (WCNC'05), New Orleans, LA, Mar. 2005.

[23] Y. Zhou, Y. Zhang, and Y. Fang, "LLK: A Link-Layer Key Establishment Scheme in Wireless Sensor Networks," Proc.2005 IEEE Wireless Commun. and Networking Conf. (WCNC'05), New Orleans, LA, Mar. 2005.

[24] W. Du et al., "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," Proc. 10th ACM Conf. Computer and Communications Security (CCS'03), Washington, DC, Oct. 2003.

[25] J. Lee and D. R. Stinson, "Deterministic Key Pre-Distribution Schemes for Distributed Sensor Networks," Proc. 11th Int'l. Wksp. Selected Areas in Cryptography (SAC'04), Lecture Notes in Computer Science, Springer-Verlag, vol. 3357/2004, 2004, pp. 184–307.

[26] J. Lee and D. R. Stinson, "A Combinatorial Approach to Key Pre-Distribution Mechanisms for Wireless Sensor Networks," Proc. 2005 IEEE Wireless Commun. and Networking Conf. (WCNC'05), New Orleans, Mar. 2005.

[27] S. A. Camtepe and B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," Proc. 9th European Symp. Research in Computer Security (ESORICS 2004), Sophia Antipolis, France, Sept. 2004.

[28] D. S. Sanchez and H. Baldus, "A Deterministic Pairwise Key Pre-Distribution Scheme for Mobile Sensor Networks," Proc. 1st IEEE Int'l. Conf. Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05), Sep. 2005.

[29] Y. Zhou and Y. Fang, "A Scalable Key Agreement Scheme for Large Scale Networks," Proc. 2006 IEEE Int'l. Conf. Networking, Sensing and Control (ICNSC'06), Ft. Lauderdale, Florida, Apr. 2006.

[30] Y. Zhou and Y. Fang, "Scalable Link-Layer Key Agreement in Sensor Networks," Proc. 2006 IEEE Military Communications Conf. (MILCOM'06), Washington, DC, Oct. 2005.

[31] Y. Zhou and Y. Fang, "A Two-Layer Key Establishment Scheme for Wireless Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 9, Sept. 2007, pp. 1009–20.

[32] D. Liu, P. Ning, and W. Du, "Group-Based Key Pre-Distribution in Wireless Sensor Networks," Proc. 4th ACM Wksp. Wireless Security (WiSe'05), Cologne, Germany, Sept. 2005.

[33] L. Zhou, J. Ni, and C.V. Ravishankar, "Efficient Key Establishment for Group-Based Wireless Sensor Deployments," Proc. 4th ACM Wksp. Wireless Security (WiSe'05), Cologne, Germany, Sept. 2005.

[34] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanism for Large-Scale Distributed Sensor Networks," Proc. 10th ACM Conf. Computer and Commun. Security (CCS'03), Washington, DC, Oct. 2003.

[35] J. Deng et al., "A Practical Study of Transitory Master Key Establishment for Wireless Sensor Networks," Proc. 1st IEEE Int'l. Conf. Security and Privacy for Emerging Areas in Commun. Networks (SecureComm'05), Sept. 2005.

[36] R. Watro et al., "TinyPK: Securing Sensor Networks with Public Key Technology," Proc. 2nd ACM Wksp. Security of Ad Hoc and Sensor Networks (SASN'04), Washington, DC, Oct. 2004.

[37] G. Gaubatz, J. Kaps, and B. Sunar, "Public Key Cryptography in Sensor Networks — revisited," Proc. 1st European Wksp.

Security in Ad Hoc and Sensor Networks (ESAS'04), Heidelberg, Germany, Aug. 2004, Revised Selected Papers, Lecture Notes in Computer Science, Springer-Verlag, vol. 3313/2005, 2005, pp. 2–18.

[38] A. Menezes, P. van Oorschot, and S. Anstone, Handbook of Applied Cryptography, CRC Press, Oct. 1996.

[39] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A RingBased Public Key Cryptosystem," Proc. ANTS III, Lecture Notes in Computer Science, Springer-Verlag, vol. 1183/1998, 1998, pp. 267–88

[40] Q. Huang et al., "Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks," Proc. 2nd ACM Int'l. Conf. Wireless Sensor Networks and Applications (WSNA'03), San Diego, CA, Sept. 2003.

[41] S. Vanstone, "Responses to NIST's Proposal," Commun. ACM, vol. 35, July 1992, pp. 50–33.

[42] J. A. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," IEEE Wireless Commun., vol 11, no. 6, Dec. 2004.

[43] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," Proc. 6th Annual ACM Int'l. Conf. Mobile Computing and Networking (MobiCom'00), Boston, MA, Aug. 2000.

[44] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proc. 33rd Hawaii Int'l. Conf. System Sciences (HICSS'00), Jan. 2000.

[45] Y. Yu, D. Estrin, and R. Govindan, Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Comp. Sci. Dept. Tech. Rep., UCLA-CSD TR-010023, May 2001.

[46] J. Newsome et al., "The Sybil Attack in Sensor Networks: Analysis and Defenses," Proc. 3rd IEEE Int'l. Symp. Information Processing in Sensor Networks (IPSN'04), Berkeley, CA, Apr. 2004.

[47] J. R. Douceur, "The Sybil Attack," Proc. 1st ACM Int'l. Wksp. Peer-to-Peer Systems (IPTPS'02), Mar. 2002.

[48] Y. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. 22nd Annual Joint Conf. IEEE Computer and Communications Societies (INFOCOM'03), San Francisco, CA, Mar. 2003.

[49] Y. Hu, A. Perrig, and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proc. 2003 ACM Wksp. Wireless Security (WiSe'03), San Diego, CA, Sept. 2003.

[50] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. 1st IEEE Int'l. Wksp. Sensor Network Protocols and Applications (SNPA'03), May 2003.

[51] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," ACM Wireless Networks, vol. 8, no. 5, Sept. 2002, pp. 331–34