A Survey on Enhancing System Performance of Wireless Sensor Network by Secure Assemblage Based Data Delivery

Conference Paper · March 2017

DOI: 10.1109/ICRAECT.2017.55

3 authors, including:

Kantharaju H C
Vemana Institute of Technology, Koramangala, Bengaluru
7 PUBLICATIONS **4** CITATIONS

SEE PROFILE

Narasimha Murthy K N
Christ University, Bangalore
22 PUBLICATIONS **29** CITATIONS

SEE PROFILE

A Survey on Enhancing System Performance of Wireless Sensor Network by Secure Assemblage based Data Delivery

Kantharaju H C
Assistant Professor, Department of CSE
Vemana Institute of Technology
Bengaluru, India
kantharajuhc@gmail.com

Dr. K N Narasimha Murthy
Professor, Faculty of Engineering,
Christ University
Bengaluru, INDIA
murthy_knn@yahoo.co.in

Abstract - To provide secure data transmission in Cluster Wireless Sensor Networks (CWSNs), the challenging task is to provide an efficient key management technique. To enhance the performance of sensor networks, clustering approach is used. Wireless Sensor Network (WSN) comprises of large collection of sensors having different hardware configurations and functionalities. Due to limited storage space and battery life, complex security algorithms cannot be used in sensor networks. To solve the orphan node problem and to enhance the performance of the WSN, authors introduced many secure protocols such as LEACH, Sec-LEACH, GS-LEACH and R-LEACH, which were not secure for data transmission. The energy consumption in existing approach is more due to overhead incurred in computation and communication in order to achieve security. This paper studies about different schemes used for secure data transmission. We are proposing new methodology called IBDS and EIBDS that will increase the performance of WSN by reducing computational overhead and also increases resilience against the adversaries.

Keywords **-** CWSNs-Cluster Wireless Sensor Networks, IBDS-Identity Based Digital Signature, Energy Efficiency, Secure data transmission, LEACH

I. INTRODUCTION

The improvement in the field of electronics and communication lead to the development in microelectronics, which reformed with the evolution of micro devices. The improvement in the field of micro devices and small chips leads to growth of WSNs-Wireless Sensor Networks with less cost, less energy consumption and efficient utilization of sensor node. A WSN is spatially scattered, self-governing nodes to observe physical and environmental conditions like heat, force, sound etc. and to direct the information to the original location through the network. Wireless sensor networks have many applications in both civilian and military such as healthcare, battlefield surveillance, traffic control and habitat monitoring. Many applications of the WSN require secure communications. The major limitation of the sensor node lies with the limited battery power, less bandwidth, limitation of size of memory [1].

In wireless communications, it is a challenging task to provide security to nodes in the network. This may be because of resource limitation on sensor nodes, Physical attacks on unused sensor node, anonymous topology, node density and size. The major Security requirements of WSNs are resource availability, message integrity, node authentication, data confidentiality and non-repudiation. These security requirements were used to provide with the requirements of scalability of network, efficient key connectivity and resilience against adversaries. Network Scalability must support large collection of sensor nodes. Efficient Key distribution mechanism must be easy to adopt for larger networks even after node deployment. Energy Efficiency involves considering both storage overhead and communication overhead on sensor nodes. In key connectivity process, same key can be shared between two or more nodes. To provide secure and efficient data transmission in WSN, data has to be encrypted and authenticated. Because of the limitation in wireless channels, adversaries may extract the information, modify it and forward the modified information to receiver. To provide better functionality in WSN, efficient key connectivity should be used [2].

II. RELATED WORK

This section discuses about the related study conducted for address security loopholes in Wireless Sensor Network.

Camtepe et al. [3] have presented an effective approach to determine how many and which keys are allotted to key set based on combinatorial design before sensor node deployment. For Secure communication two node may have common key in key-chains and they linked with each other via key path. A common key is shared between each pair of neighboring nodes via key path. The authors have presented Balanced Incomplete Block Design (BIBD) approach which uses Symmetric design and to generate key chains a Generalized Quadrangles (GQ) is used. The use of Symmetric design provides efficient key sharing mechanism compare to probabilistic algorithms by sacrificing the resilience against compromised nodes. In GQ design, each node is assigned K keys from key pool P. For fixed block size, GQ provides

978-1-5090-6701-5/17 $31.00 © 2017 IEEE
DOI 10.1109/ICRAECT.2017.55

highest number of blocks and for fixed number of blocks, GQ provides smallest block size, which is not a scalable solution.

Ren et al [4] suggested a framework for distribution of keys that provides authentication for node-to-node and node-to-sink along with the report forwarding routes. The authors introduced an algorithm called Location aware End-to-end Data Security (LEDS), where set of keys are stored in each node based on its own location and secret keys were limited to its geographical locations. In LEDS, each sensor node has a one public key, distributed to all hops in a cluster and a distinct private key know to itself. Each node stores single authentication key for report authorization cell. Based on the relative position of the sink node, each node selects total number of report authorization cells. The main aim of LEDS is to mitigate the impact of malicious nodes without affecting end to end security and to guarantee against dos attacks. LEDS introduces additional overhead in message and false detection report, which incurs extra energy consumption in computation as well as communication.

Xuan Hung Le et al. [5] introduced an approach called Energy-efficient Access control scheme Based on eLliptic curvE cryptography (ENABLE) to overcome problems of mutual authentication, Denial of service attacks and more importantly to enhance energy efficiency. Here Key agreement is done using Elliptic Curve Diffie Hellman (ECDH) between KDC and sensor nodes. Private Key algorithm uses KCDH that allows two parties to establish shared secret key. To avoid security attacks, shared secret keys are renewed frequently. The major limitation of ENABLE is overhead incurred in key exchange, encryption and decryption will reduce the performance a sensor node.

Maarouf et al. [6] have proposed a solution, Efficient Monitoring Procedure In a REputation system (EMPIRE) for trust-aware routing, which limits the periodic observations on node by preserving the caliber to notify the attacks at an acceptable level. Monitoring efficiency is determined by Nodal Monitoring Activity (NMA) in association with performance parameters. In EMPIRE, each node changes the states (ON and OFF) between two NMAs. In ON state Nodal Monitoring Activities validate the events like header validation, over hearing packets and storing packets. In OFF state, no monitoring activities, only send, receive and processing data. EMPIRE consumes more energy, because of increasing routing trust awareness parameter (β). So, to guarantee less power consumption, optimum values of β meets delivery ratio at low level of NMA.

Chia-Mu Yu et al. [7] have presented ConstrAined Random Perturbation-based pairwise keY establishment (CARPY) scheme and its variant, a CARPY+ scheme, for WSNs. It is first non-interactive key establishment scheme that provides great resilience against the node compromised attacks, designed for WSNs. CARPY scheme has two steps, the offline step, before sensor node deployment to check desired key length, selection of parameters and preinstalling keys to sensor node. In online step, Pair wise key is necessary to setup for each pair of sensor nodes. In CARPY+, no communication is required to establish pairwise key, key establishment procedure will not disrupt by routing layer attacks there by slightly reduces overhead in communication. CARPY+ provides great resilience against node compromising and becomes first non-interactive key establishment scheme. The CARPY is not resilient against attacks in network layer, Overhead in computation of CARPY+ is more than CARPY.

Wenjum .Gu et al. [8] have presented protocol for secure end to end. Specifically, this protocol is based on differentiated key pre-distribution. The major aim here is to generate the keys randomly and distribute to all the sensor nodes in the network to safeguard against the adversaries. Keys are pre-distributed to all nodes in the network to enhance resilience. Differentiated key pre-distribution consists of two phases, key pre-distribution and pairwise key establishment. In key pre-distribution phase, a unique keys are allocated from the key pool. In pairwise key establishment, after deployment of keys, nodes will start discovering neighbors and obtains key IDs of neighbors. GPSR is used to provide secure communication at end to end level, which allows each node to assign weight of all its secure neighbors (pairwise key established with neighbors) that are nearer to sink node rather than itself. The attack against the nodes which were having large pre-distributed keys might lead to attack at high level. To avoid attack on nodes having more keys, camouflaging technique is used. The idea here is, Nodes having large number of pre-distributed keys are hide and resulting attacker cannot identify the nodes which were having more keys. But this approach leads to additional communication overhead, thereby reduces the efficiency of WSN.

Daojing He et al. [9] have proposed a DiCode protocol, which has the ability to resist Dos attacks against network availability. DiCode has two participants, proxy signer and an original signer. Original signer specifies the identity of the proxy signer, range of messages to sign and expiration time. Proxy signatures are generated by Proxy signer with the help of proxy signature keys provided by original signer. Dicode has three levels. In System Initialization level, owner generates private and public keys which were delivered to authorized users. Before deployment, only public key of network owner is loaded on each node. In user Pre-processing, level code dissemination packets are constructed and sends them to every node. In verification level, RSA algorithm is used to provide resilience against dos attacks. DiCode has low impact on delay and also energy overhead remains similar to that of Selgue or Deluge.

Jokhio et al. [10] have presented a technique called SCADD, enhances the security in WSN by providing an effective approach for solving the attacks against compromising the node and attacking the node. SCADD comprises of two blocks to identify attacks, Node Attack Detection (NAD) to check node is attacked or about to be attacked. NAD uses two types of beacons, alert beacon is communicated when false node attempt to communicate or when severity is minimal, and red beacon is used when attack is severe is high, which leads to node capture attacks. When severity is high, sensor activates

DAM which takes defensive measures to handle the attack. Before deployment, each sensor node contains VMAT table that contains information such as private/public keys, Locations of neighbors, routing information table etc. In DAM, to overwritten zero in place of information bits, thereby avoiding false node to get access to memory locations, self – destruction algorithm is used. The algorithm is intended to erase all vital information in VMAT, which may affect the network or overall performance of the network. SCADD protocols incurs communication and processing overheads.

Abdoulaye Diop et al [11] have proposed ESKMS for hierarchical clustering networks to provide secure and efficient key management technique. This technique allocates the keys within a cluster competently and updates the pre-deployed keys regularly to avoid the node compromising attack. Here, two kinds of keys are used for key management. Network key is global shared key used by nodes in the network and base station for encrypting messages and to transmit to each and every sensor nodes in the network. Network keys are programmed into memory just before the deployment and is valid for limited period. Pair-wise keys are used between two parties to establish unique pair-wise keys. During initialization phase and formation of cluster, pairwise keys are set dynamically. ESKMS consist of five phases. In Key-Predistribution, secret keys are loaded to sensor nodes before deployment and shared with BS. In Pair-wise key establishment, to provide secure communication in sensor network, pair wise keys are allocated by base station. BS uses Network key, generates MAC and broadcast these information along with nonce to all sensor nodes. In Data Transmission phase, nodes send encrypted data packets. In key updating Phase, to reduce attacks on nodes, network keys are updated periodically. In Re-clustering phase, based on energy available in sensor node, each node get a chance to become a cluster head and CH rotated at regular interval of time. In EKMS, there is slightly more computation overhead and storage overhead for storing network key, Encryption key, Pair-wise key, Key updation and reclustering.

Huanf Lu et al. [12] have proposed SET-IBS and SET-IBOOS which are secure and efficient data transmission techniques, where clusters are formed vigorously and periodically. Security in SET-IBS in pairing domain relies on complexity of Diffie Hellman problem. Security in SET-IBOOS, depends on discrete logarithm problem. To provide security, key management technique is used. To minimize the computational cost, storage cost and to provide authentication to message packets for efficient communication, digital signatures are used. Security in SET-IBS depends on Identity Based cryptography, where ID is based on public keys. So, to ensure efficient communication and to conserve energy of sensor node, users obtains private keys without auxiliary data transmission. SET-IBOOS is based on private key cryptography in order to solve the orphan node problem. SET-IBS, SET-IBOOS protocols incurs faster energy consumption due to the overhead in computation and communication.

Karuna Babber et al.[13] have proposed Energy Efficient Uniform-clustering Algorithm (EEUA) to form uniform clusters, to select cluster heads and to provide secure transmission of data for energy efficiency. Uniform clusters are formed by splitting sensing area into any defined angle, accordingly clusters are formed. For each cluster, cluster head is selected based on mean distance of sensor nodes with in a cluster from the center location. To provide security in data transmission, encryption and decryption of data is performed using general version of substitution ciphering. To carry out multiple character substitution ciphering, paly fair technique is used. The security mechanism used here for encryption and decryption is very simple, adversaries may easily compromise the node.

Camtepe et al. [3] have presented an effective approach to determine how many and which keys are allotted to key set based on combinatorial design before sensor node deployment. For Secure communication two node may have common key in key-chains and they linked with each other via key path. A common key is shared between each pair of neighboring nodes via key path. The authors have presented Balanced Incomplete Block Design (BIBD) approach which uses Symmetric design and to generate key chains a Generalized Quadrangles (GQ) is used. The use of Symmetric design provides efficient key sharing mechanism compare to probabilistic algorithms by sacrificing the resilience against compromised nodes. In GQ design, each node is assigned K keys from key pool P. For fixed block size, GQ provides highest number of blocks and for fixed number of blocks, GQ provides smallest block size, which is not a scalable solution.

Ren et al. [4] have presented a framework for key management which provides authentication for node-to-node and node-to-sink along with the report forwarding routes. The authors introduced an algorithm called LEDS-Location-aware End-to-End Security, where each node stores a set of keys based on its own location and secret keys were limited to its geographical locations. In LEDS, each sensor node has a one cell key (public key), shared to all nodes in the cluster and a unique secret key that is only know to itself. Each node stores one authentication key for report authorization cell. Based on the relative position of the sink node, each node selects total number of report authorization cells. The main aim of LEDS is to mitigate the impact of compromised nodes without affecting end to end security and to guarantee against dos attacks. LEDS introduces message overhead and en-route filtering operations, incur extra energy consumption in computation as well as communication.

Xuan Hung Le et al. [5] have presented an energy efficient access control scheme based on Elliptic Curve Cryptography (ENABLE) to overcome problems of mutual authentication, Denial of service attacks and more importantly to provide energy efficiency. Here Key agreement is done using Elliptic Curve Diffie Hellman (ECDH) between KDC and sensor nodes. KCDH allows two parties to establish shared secret key that are used for private key algorithms. To avoid security attacks, shared secret keys are renewed frequently. The major

limitation of ENABLE is overhead incurred in key exchange, encryption and decryption will reduce the performance a sensor node.

Maarouf et al. [6] have proposed a solution Efficient Monitoring Procedure In a REputation system (EMPIRE) for trust-aware routing, which is a probabilistic and distributed monitoring methodology that tries to reduce the monitoring activities per node by preserving the ability to detect attacks at an acceptable level. Monitoring efficiency is determined by Nodal Monitoring Activity (NMA) in association with performance parameters. In EMPIRE, each node changes the states (ON and OFF) between two NMAs. In ON state Nodal Monitoring Activities validate the events like header validation, over hearing packets and storing packets. In OFF state, no monitoring activities, only send, receive and processing data. The EMPIRE consumes more energy, if we increase routing trust awareness parameter (β). So, to guarantee less power consumption, optimum values of β meets delivery ratio at low level of NMA.

Chia-Mu Yu et al. [7] have presented ConstrAined Random Perturbation-based pairwise keY establishment (CARPY) scheme and its variant, a CARPY+ scheme, for WSNs. It is first non-interactive key establishment scheme that provides great resilience against the node compromised attacks, designed for WSNs. CARPY scheme has two steps, the offline step, before sensor node deployment to check desired key length, selection of parameters and preinstalling keys to sensor node. In online step, each pair of sensor nodes finds the pairwise key. In CARPY+, no communication is required to establish pairwise key, key establishment procedure will not disrupt by routing layer attacks there by slightly reduces overhead in communication. CARPY+ provides great resilience against node compromising and becomes first non-interactive key establishment scheme. The CARPY is not resilient to routing layer attacks, Computation overhead of CARPHY+ is slightly larger than CARPY.

Wenjum Gu et al. [8] have designed an end to end secure communication protocol. Specifically, this protocol is based on a methodology called differentiated key pre-distribution. The idea behind is to distribute the randomly generated keys to different sensors to protect against the adversaries. Keys are pre-distributed to all nodes in the network, by which it will enhance the resilience. Differentiated key pre-distribution consists of two phases, key pre-distribution and pairwise key establishment. Key pre-distribution assigns unique keys randomly from the key pool. In pairwise key establishment, once keys are pre-distributed and deployed, nodes will start discovering neighbors and obtains key IDs of neighbors. GPSR is used to provide end to end secure communication, which allows each node to assign weight of all its secure neighbors (pairwise key established with neighbors) that are closer to sink node rather than itself. The capture of nodes with large number of pre-distributed keys might lead to higher attack impact. To avoid attack on nodes having more keys, camouflaging technique is used. The idea here is to hide the nodes with more pre-distributed keys resulting attacker cannot distinguish the nodes with more keys and others. But this approach costs extra communication overhead, thereby reduces the efficiency of WSN.

Daojing He et al. [9] have proposed a DiCode protocol, which has the ability to resist Dos attacks against network availability. DiCode has two participants, proxy signer and an original signer. Original signer specifies the identity of the proxy signer, range of messages to sign and expiration time. Proxy signer generates proxy signatures using proxy signature keys which is provided by original signer. Dicode has three levels namely System Initialization, user Pre-processing and sensor node verification. In system initialization level, the owner creates public and private keys which is delivered authorized users. Before deployment, only network owner's public key is loaded on each node. In user Pre-processing level code dissemination packets are constructed and sends them to every node. In verification level, RSA algorithm is used to provide resilience against dos attacks. DiCode has low impact on delay and also energy overhead remains similar to that of Selgue or Deluge.

Jokhio et al. [10] have presented a technique called SCADD, enhances the security in WSN by providing an effective approach for solving the node compromise attack and node capture attacks. SCADD protocol comprises of two blocks namely Node Attack Detection (NAD) and Defense Advocating measure (DAM) block. NAD block identifies whether node is compromised or not compromised. NAD uses two types of beacons, alert beacon is communicated when false node attempt to communicate or when severity is minimal and red beacon is used attack is severe which leads to node capture attacks. When severity is high, sensor activates DAM which takes defensive measures to handle the attack. Before deployment, each sensor node contains VMAT table i.e Vital Memory Address Table that contains information such as cryptographic keys, neighbor locations, routing table information etc. In DAM, to overwritten zero in place of information bits, thereby avoiding false node to get access to memory locations, self – destruction algorithm is used. The algorithm is intended to erase all vital information in VMAT, which may affect the network or overall performance of the network. SCADD protocols incurs communication and processing overheads.

Abdoulaye Diop et al [11] have proposed ESKMS for hierarchical clustering networks to provide secure and efficient key management technique. This technique allocates the keys within a cluster competently and updates the pre-deployed keys regularly to avoid the node compromising attack. Here, two kinds of keys are used for key management. Network key which is global shared key used by nodes in the network and base station for encrypting messages and to broadcast to all other sensor nodes in the network. Network keys are programmed into memory just before the deployment and is valid for limited period. Pair-wise keys are used between two parties to establish unique pair-wise keys. During initialization phase and formation of cluster, pairwise keys are set dynamically. ESKMS consist of five phases namely Key

Predistribution phase, Pair-wise key establishment, Data Transmission phase, Key Updating phase and Re-clustering phase. In Key-Predistribution phase, secret keys are loaded to sensor nodes before deployment and shared with BS. In Pair-wise key establishment, to provide secure communication in sensor network, pair wise keys are allocated by base station. BS uses Network key, generates MAC and broadcast these information along with nonce to all sensor nodes. In Data Transmission phase, nodes send encrypted data packets. In key updating Phase, to reduce attacks on nodes, network keys are updated periodically. In Re-clustering phase, based on energy available in sensor node, each node get a chance to become a cluster head and CH rotated at regular interval of time. In EKMS, there is slightly more computation overhead and storage overhead for storing network key, Encryption key, Pair-wise key, Key updation and reclustering.

Huanf Lu et al.[12] have proposed SET-IBS and SET-IBOOS which are secure and efficient data transmission techniques, where clusters are formed vigorously and periodically. Security in SET-IBS in pairing domain relies on hardness of Diffie Hellman problem. Security in SET-IBOOS, depends on discrete logarithm problem. To provide security, key management technique is used and to minimize the computational cost, storage cost and to provide authentication to message packets for efficient communication, digital signatures are used. Security in SET-IBS depends on Identity Based cryptography, where ID is based on public keys. So, to ensure efficient communication and to conserve energy of sensor node, users obtains private keys without auxiliary data transmission. SET-IBOOS is based on symmetric key cryptography in order to solve the orphan node problem. Here, there may be a possibility of revealing public key and secret key by compromised node, thereby reducing security of node.

Karuna Babber et al.[13] have proposed Energy Efficient Uniform-clustering Algorithm (EEUA) to form uniform clusters, to select cluster heads and to provide secure transmission of data for energy efficiency. Uniform clusters are formed by splitting sensing area into any defined angle, accordingly clusters are formed. For each cluster, cluster head is selected based on mean distance of sensor nodes with in a cluster from the center location. To provide security in data transmission, encryption and decryption of data is performed using general version of substitution ciphering. To carry out multiple character substitution ciphering, paly fair technique is used. The security mechanism used here for encryption and decryption is very simple, adversaries may easily compromise the node.

III. SUMMARY OF SECURE DATA TRANSMISSION PROTOCOLS

Authors	Findings	Results	Limitations
Camtepe et al.	Prior to deployment, Keys must be distributed from Key Pool.	BIBD and GQ provides Efficient key sharing using Symmetric design	No Resilience against compromised nodes and not scalable.
Ren et al.	Vulnerable to Node Compromise attack and DoS Attacks	LEDS, Provides authentication for node to node and node to sink and also robust against DoS attacks	Computation overhead and communication overhead incurs extra energy consumption.
Xuan Hung Le et al.	ECC limits the security, no Mutual authentication and susceptible to DoS Attacks	ENABLE, uses public key cryptography to provide Mutual authentication and defend against DoS attack.	ECDH increases computation overhead and since, Shared Keys are renewed frequently, which requires additional energy consumption
Maarouf et al.	To ensure trust-aware routing, node are monitored continuously to identify misbehavior events which is costlier because of resource scarcity.	EMPIRE uses NMA that tries to reduce the monitoring activities of each node by preserving the capability to identify attacks at an acceptable level.	Increasing routing trust awareness improves delivery ratio but significantly increases power consumption
Chia-Mu Yu et al.	Key Establishment schemes which were proposed are inefficient against security and high energy consuming due to involved communications.	CARPHY, offline step is performed before sensor node deployment and preinstalls keys. Pairwise key establishment is used in online step when sensor nodes are deployed.	CARPY is not resilient to routing layer attacks. Computation overhead in CARPHY+ is slightly larger than CARPY.
Wenjum Gu et al.	Every sensor node is deployed with identical number of keys which makes link more robust during end to end communication. Providing more	DKP mechanism is used to distribute diverse keys to different sensors to protect against the adversaries. Keys are predistributed to all nodes in the network,	This approach costs extra communication overhead which will reduces the efficiency of WSN

	keys into each node may enable the attacker to try to reveal the keys during attack, which may compromise the resilience of the link.	distributing more keys to few nodes will enhance the resilience. To avoid attack on nodes having more keys, camouflaging technique is used.	
Daojing He et al.	Most of the code dissemination protocols are based on centralized approach, which allows base station to initiate code dissemination. The centralized approach is not scalable, vulnerable to attacks and also inefficient.	DiCode uses three phases such as initialization, user preprocessing and verification. In initialization, original signer creates its public and private keys and signature keys to authorized users. Preprocessing phase constructs code dissemination packets. Verification phase allows nodes to accept packets if verification succeeded.	DiCode has low impact on delay and also energy efficiency is not improved when compared to Selgue and Delgue.
Jokhio et al.	For Secure communication in WSN, tamper resistant nodes increases the network cost tremendously. Destroying legitimate nodes by erasing its memory may damage WSN.	SCADD provides cost effective solution against node capture attacks and compromise attacks by using NAD and DAM block mechanisms.	When attack severity is low NAD is used. When severity is high NAD activates DAM, erases VMAT which includes crypto keys, neighbor locations, routing information. SCADD incurs communication and processing overheads.
Abdoulaye Diop et al	Security protocols such as LEACH, Sec-LEACH and GS-LEACH were exposed to key collision attacks and does not provide full connectivity	ESKMS distributes and update the keys at regular interval of time by using hashing technique. Data encryption and MAC to protect against the node compromise attack from malicious node.	More computation overhead and storage overhead for storing network key, Encryption key, pair-wise key, Key updation and reclustering. Thus, reduces life time of sensor node.
Huanf Lu et al.	Symmetric key management for security does not share pairing keys with neighbors. Further, orphan node problem reduces node joining with CH which increases transmission overhead and also system energy consumption.	To provide security in data transmission, SET-IBS, SET-IBOOS uses IBS scheme to validate encrypted sensed data by using digital signature to messages, which eliminates orphan node problem. SET-IBS is efficient mechanism for data communication and conserves energy. SET-IBOOS reduces computation overhead for enhancing security.	Both protocols consume more energy of sensor node because of communication and computation overhead in achieving security.
Karuna Babber et al.	The secure protocols such as LEACH, PEGASIS, TEEN, HEED does provide energy efficiency as distance of transmission increases.	EEUA forms uniform clusters, to select cluster heads and to provide secure transmission of data for energy efficiency.	Security mechanism used for encryption and decryption is very simple, adversaries may easily compromise the node.

IV. SYSTEM DESCRIPTION AND METHODOLOGY

The prime intention of this preliminary study phase is to understand the effectiveness in the techniques proposed by various researchers and draw a conclusion of concrete research gap and open issues of security of wireless sensor network. This phase will add much information acting as guidelines to carry our further research direction to accomplish the goal of the study for reducing overhead of security protocols and strengthening robustness.

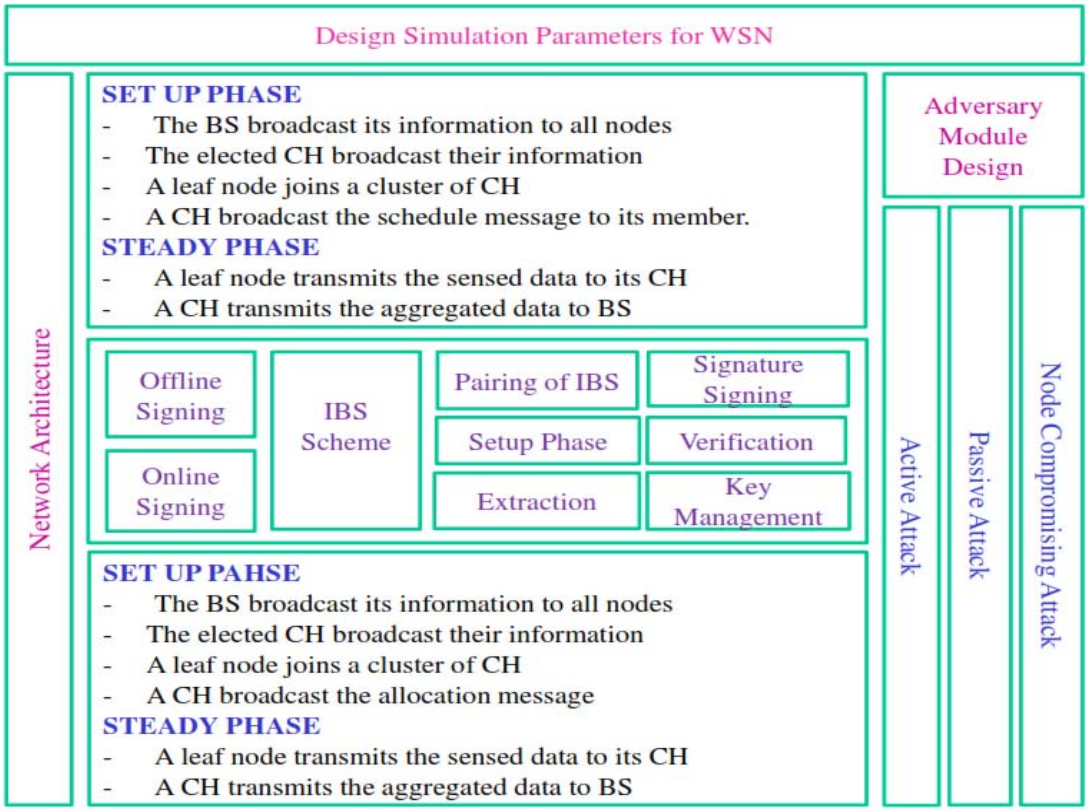

Fig. 1: Architecture of Proposed System

In Network Architecture, the Cluster Wireless Sensor Networks (CWSN) consists of large set of sensor nodes with fixed base station (BS). Each sensor node in CWSN, consumes more energy for data sensing, processing and transmission. To limit the energy consumption, the cluster head (CH) aggregates the data and sends it to base station. Generally, sensor nodes switches to sleep mode automatically to avoid power consumption.

To provide security and efficiency in data transmission, protocols IBDS and EIBDS for wireless sensor network were used to identify both online and offline interaction vulnerabilities from the adversary by using identity based cryptography scheme. The idea of proposed system is to use the digital signature to message packets, to perform authentication of the encrypted data, which provides efficient communication. Further, to ensure security, key management scheme is used. In the proposed work, base station initially preloads secret keys and pairing parameters, which overcomes problem of key escrow.

The proposed study for secure communication is based on identity based cryptography, in which public keys are used as their identity information. Thus, without auxiliary data transmission, users can obtain the corresponding private keys, which becomes efficient in communication and conserves energy.

To reduce overhead in computation, to increase security in the network and to solve orphan node problem symmetric key cryptography is used. The proposed protocols concentrates on security requirements for secure transmission and analysis against attacking models such as active attacks, passive attacks and node compromising attacks.

In the proposed work, during communication, protocol consists of set-up phase and a steady-state phase and initialization of nodes operates in rounds before node deployment. The online mode and offline mode will operate in multiple rounds during communication, and based on the decision taken locally, self-elected aggregator nodes are selected without additional data transmission. The offline mode does not use any secret information for signing.

The proposed framework provides secure data transmission for wireless sensor network with concrete identity based settings, which uses identity information and digital signature for authentication and verification. Comparing to existing techniques, proposed system will consume less energy for computation and storage. In the proposed system, computation overhead will be less which will be more suitable for node-to-node communications.

Finally security analysis is done based on Node compromising attack, passive attack, and active attack and compared with LEACH [14] algorithm for benchmarking purpose.

V. POSSIBLE OUTCOMES

The possible outcome of the study is as follows:

- Enhanced Node Lifetime (the time of FND) – FND, denotes the duration of the sensor node that is fully functional in network. Therefore, to extend the life time of the network, we are maximizing time of FND.
- Good number of alive nodes – The nodes that have not failed (dead) used to sense and collect the information in a WSN. Therefore, improving the number of alive nodes will increase the performance of the network.
- Optimality in Total system energy consumption - Energy consumption of proposed approach will be less compared with LEACH.

VI. CONCLUSION

In this paper, we have studied different security approaches for secure data transmission in Cluster Wireless Sensor Networks. The deficiency in existing security approaches has been addressed. The proposed secure and efficient data transmission protocol IBDS and EIBDS, will provide better efficiency by reducing computation overhead and increases security against adversaries.

REFERENCES

[1] . Z. Zhang and V. Varadharajan, "Wireless Sensor Network key management survey and taxonomy", Journal of Network and Computer Applications, vol 33, pp 63-75, 2010.

[2] . Z. J. Haas, L. Yang, M-L. Liu, Q. Li, and F. Li, "Current Challenges and Approaches in Securing Communications for Sensors and Actuators," Chapter 17 in "The Art of Wireless Sensor Networks," H.M. Ammari (ed.), Springer-Verlag Berlin Heidelberg, 2014, DOI: 10.1007/978-3-642-40009-7_17.

[3] . Camtepe, S.A., Yener, B., "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", IEEE/ACM Transactions on Networking, Vol. 15, No. 2, April 2007.

[4] . Ren, K., Lou, W., Zhang, Y., "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 7, No. 5, May 2008.

[5] . Xuan Hung Le, Sungyoung Lee, Ismail Butun, Murud Khalid, Ravi Shankar, Miso Kim, manhyung Han, young-Koo Lee and Heejo Lee, "An Energy Efficient Access Control Scheme for Wireless Sensor Networks based on Elliptic Curve Cryptography", Communication and Networking, Vol 11, No. 6, December 2009.

[6] . Maarouf, I., Baroudi, U., Naseer, A.R., "Efficient monitoring approach for reputation system based trust-aware routing in wireless sensor networks", IET Communications, 2008, Vol. 3, Iss.5, pp.846-858, October 2008.

[7] . Yu, C.M., Lu, C.S., Kuo, S.Y., "Non-interactive Pairwise Key Establishment for Sensor Networks, IEEE Transactions on Information Forensics and Security", Vol. 5, No. 3, September 2010.

[8] . Wenjun Gu, Neelanjana Dutta, Sriram Chellappan and Xiaole Bai, "Providing End-to-End Secure Communications in Wireless Sensor Networks, IEEE Transactions on Network and Service Management", Vol. 8, No. 3, September 2011.

[9] . Daojing He, D., Chen, C., Chan, S., Bu, J., "DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks", IEEE Transactions on Wireless Communications, Vol. 11, No. 5, May 2012.

[10] .Jokhio, S.H., Jokhio, I.A., Kemp, A.H., "Node capture attack detection and defense in wireless sensor networks", IET Wireless Sensor Systems, Vol 2, Iss 3, pp 161-169, Oct 2012.

[11] .Abdoulaye Diop, Yue Qi, Qin Wang, Shariq Hussain "An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks", International Journal of Computer and Communication Engineering, Vol 1, No 4, pp 365-370, Nov 2012.

[12] .Huanf Lu, Jie Li, Mohen Guizani "Secure and Efficient Transmission for Cluster-based Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Vol 25, Iss 3, pp 750-761, 2014.

[13] .Karuna Babber, Rajneesh Randhawa "Energy Efficient Clustering with Secured Data Transmission Technique for Wireless Sensor Networks", International Conference on Computing for Sustainable Global Development, pp 3023-3025, 2016.

[14] .W. Heinzelman, A. Chandrakasan and H. balakrishnan, "An Application Specific protocol architecture for Wireless Micro Sensor Networks", IEEE transactions on Wireless communications, vol 1, no.4, pp. 660-670, oct 2002.