Volume 5, Issue 9, September 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Energy Consumption and Secure Multipath Routing in Cluster Based Wireless Sensor Network

Payal Machirkar, Nita Thakare, Animesh Tayal
Department of Computer Science and Engineering
PCE, Nagpur, Maharashtra, India

Abstract— Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. Proposed a CRP for secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. CRP uses digital signature (DSI) scheme and the identity-based online/offline digital signature (DSOO) scheme, for security. In DSI security relies on the hardness of the Diffie-Hellman problem in the pairing domain so that it uses the hashing technique for signing and verification. In DSOO it reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. To improve the performance if the system Energy aware Rule based scheme was proposed.Simulation results shows that proposed system has better performance compared with the existing system in terms of security, efficiency, energy consumption.

Keywords— digital signature scheme, AODVrouting protocol

I. INTRODUCTION

A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radiotransceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

Compared with flat routing protocols in WSNs, clustering routing protocols have a variety of advantages, such as more scalability, less load, less energy consumption and more robustness. In this section, we summarize these advantages as well as the objectives of WSN clustering as follows:

1. More Scalability
2. Maximizing of the Network Lifetime

II. RELATED WORK

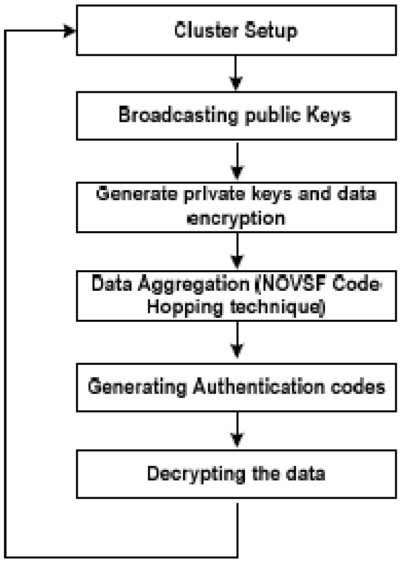
The number of literatures specifically targeted to security of WSNs has grown significantly. Here , we provide a sample of studies based on cryptographic methods, and focus on those targeted to access control for WSN.

Adrian Carlos Ferreira et al.[3] focused on adding security to cluster-based communication protocols in homogeneous WSNs with resource-constrained sensor nodes. The auther tells about the SLEACH, the first modified version of LEACH with cryptographic protection against outsider attacks. It prevents an intruder from becoming a CH or injecting bogus sensor data into the network. SLEACH is quite efficient, and preserves the structure of the original LEACH, including its ability to carry out data fusion. The simplicity of our solution relies on LEACH's assumption that every node can reach a BS by transmitting with sufficiently high power.

Zhou Ruyan, Chen Ming et al. introduces the the cluster-based routing protocols for wireless sensor network based on genetic clustering algorithm. In the network of non-uniform distribution nodes, this method can select the cluster heads after setting the nodes. During the operation of the WSN, when the geographic location change or failure of cluster heads, WSN need to be re-cluster or reselecting the cluster heads, the method proposed in the paper can be used. By using this method, the scientific and rational treatment results can be gotten, which has important practical ignificance in balancing the network energy and extending the network life cycle[4].

Vishnu Kumar et al. [5] proposed a cluster based sensor network consist hundreds of small sensor node, each node has the sensing ability with less computational and communication power. Even though Sensor node has a basic hardware and software for manipulating the given task This paper presents a secure energy efficient dynamic routing scheme (SEEDR) for wireless sensor networks. SEEDR uses a symmetric cryptography algorithm to support security. The dynamic key exchange protocol based on DH (Diffie-Hellman) algorithm is proposed, with non-blocking OVSF codes.

Conceptual process of the algorithm is illustrated in figure.1 (a). Attackers cannot decrypt the information unless the private key is known. Using the public key the attackers cannot generate the private key.


Cluster Setup
Broadcasting public Keys
Generate private keys and data encryption
Data Aggregation (NOVSF Code Hopping technique)
Generating Authentication codes
Decrypting the data

(a)

Figure 1. (a) Conceptual flow of the SEEDR algorithm

In this paper, authers mainly present the design of Secure-EEDR, a secure energy efficient dynamic routing protocol. The core idea of our protocol is derived by using Diffie-Hellman algorithm with NOVSF code-Hopping technique which not only provides a variety of security features, but also increase the efficiency of the entire network in terms of energy. It has been proved by simple analysis that our algorithm needs less storage, communication cost and computation power which makes the network more stable and secured.

I-Hsun Chuang et al gaves the A resource-efficient key management protocol which was essential for security-sensitive applications in wireless sensor networks (WSN). Moreover, the dynamic pair-wise key and group key management protocols are also important for long-lived and mobile WSN. In this paper, a Two-layered Dynamic Key Management (TDKM) approach for cluster-based WSN (CWSN) is proposed. Both pair-wise key and group key are distributed in three rounds for key material exchange without encryption/decryption and exponentiation operations in TDKM. In theoretical analysis, TDKM is compared with other key management protocols to show its efficiency.

The performance of TDKM is analyzed and compared with other group key management protocols [6] in several performance metrics including rounds, computation overhead, number of messages, and message size. The notations used for performance comparison are listed as follows:

1. n: the number of GMs in the group,
2. i: the index of GM,
3. OH(): the complexity of hash operation,
4. ODec(): the complexity of decryption operation,
5. OEnc(): the complexity of encryption operation,
6. OExp(): the complexity of exponentiation operation,
7. OMul(): the complexity of multiplication operation,
8. ODiv(): the complexity of division operation.

This paper contains the the two-layered dynamic key management (TDKM) approach was proposed for cluster-based wireless sensor networks. In fact, this technique was easily applied to multi-level network architecture. By comparing TDKM with tree-based approaches, no encryption/decryption operation was required to transmit the materials of group key in TDKM. By comparing TDKM with contribution-based approaches, multiplication operation instead of exponentiation operation was used to generate group key. Moreover, the total round of group key generations is constant and the computational complexity is O(n2) for TDKM. Furthermore, the simplified TDKM was also proposed to enhance the system performance. For simplified TDKM, GL only needs to perform O(n) hash operations to transmit the materials of group key and each GM only needs to perform constant times of hash operations to generate the group key. Finally, the relationships between system performance and the number of groups are analyzed[6].

P. Nuir et al [7] presented an Energy-efficient and Secure Pattem-based Data Aggregation protocol (ESPDA) for wireless sensor networks. ESPDA was energy and bandwidth efficient because cluster-heads prevent the transmission of redundant data from sensor nodes. ESPDA was also secure because it does not require the encrypted data to be decrypted by cluster-heads to perform data aggregation. In ESPDA, cluster-head first requests sensor nodes to send the corresponding pattern code for the sensed data. If multiple sensor nodes send the same pattern code to the cluster-head, then only one of them is permitted to send the data to the cluster-head. Hence, ESPDA has advantages over the conventional data aggregation techniques with respect to energy, bandwidth efficiency and security. Simulations results show that as data redundancy increases, the amount of data transmitted from sensor nodes to cluster-head decreases up to 45% when compared to conventional algorithms.

This paper proposes an Energy-efficient and Secure Patten based Data Aggregation protocol (ESPDA) for cluster-based wireless sensor networks. Knowing that 70% of the energy consumption was due to data transmission [3], the proposed ESPDA reduces data transmission by not sending the redundant data from sensor nodes to cluster-heads. Since the number of sensors in a sensor network was very large, often various sensors detect common data. Data aggregation [4] is used to eliminate redundancy and minimize the number of transmissions in order to save energy. In conventional data aggregation methods, cluster-heads receive all the data from sensor nodes and then eliminate the redundancy by checking the contents of the data as shown in Figure l(b). In ESPDA, instead of transmitting the entire data with redundancy, the sensor nodes send the corresponding pattern codes to cluster-head for data aggregation. Thus, data aggregation is performed even before the actual data is transmitted from the sensor nodes as illustrated in Figure l(c).

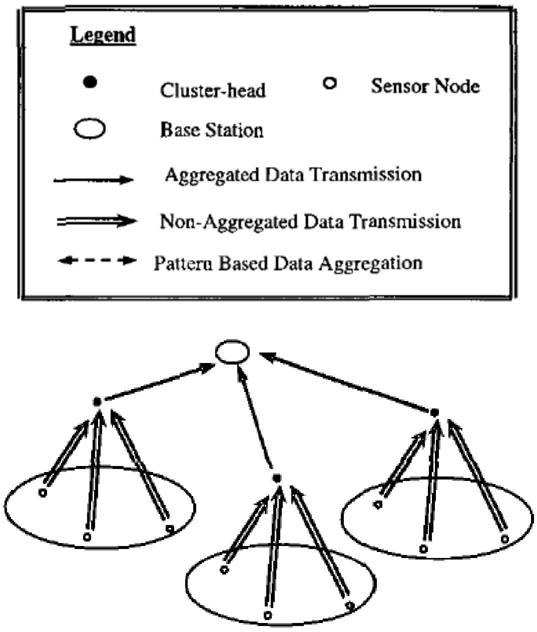

Legend
Cluster-head
Sensor Node
Base Station
Aggregated Data Transmission
Non-Aggregated Data Transmission
Pattern Based Data Aggregation

Figure l (b). Data Transmission using conventional data aggregation.

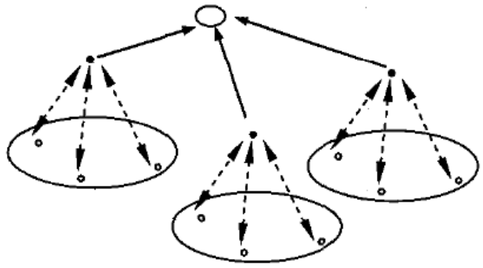


Figure I(c). Data Transmission using ESPDA technique

This paper has introduced an energy-efficient and secured data aggregation protocol called ESPDA. In contrast to Conventional data aggregation protocols ESPDA avoids the transmission of redundant data from the sensor nodes to the cluster-head. To make the data transmission and aggregation more secured cluster-head is not required to decrypt or encrypt the data received from the sensor nodes. The symmetric keys that are used due to their low memory space and computing requirements, are not transmitted between the cluster-head and the sensor nodes. Simulation results show that ESPDA improves the energy and bandwidth efficiency the protocol reduces the number of packets transmitted. Thus when ESPDA is integrated with our previously proposed security protocol it greatly helps to achieve the primary goal of energy efficiency and security essential in wireless sensor networks[7].

Seppo Virtanen[8], evaluate and compare the performance of A-GF standard GF in terms of three metrics such as data transmission rate, the average route length and the total network traffic in A-GF. All these three methods for the final result. During each run, the source node sent packets to the sink ode at a rate of 1 packet/second for 200 seconds. Figure 1(d) shows that the data transmission success of A-GF and GF are comparable whenonly 5% of the links in the network are symmetric. However , in case of 20% of link asymmetric in the network. This shows the better performance than GF (96% over 90%). Figure 1(f) shows the Average route length of data transmission rate and the figure 1(e) shows that the Total traffic network of data transmission.

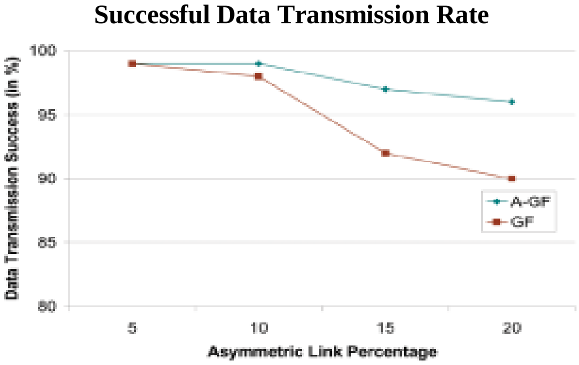


Figure 1(d). Data transmission success

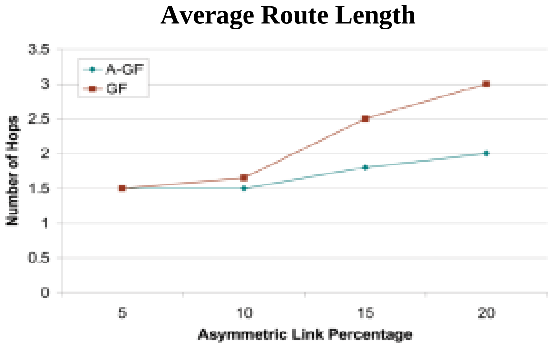


Figure 1(e).Average route length

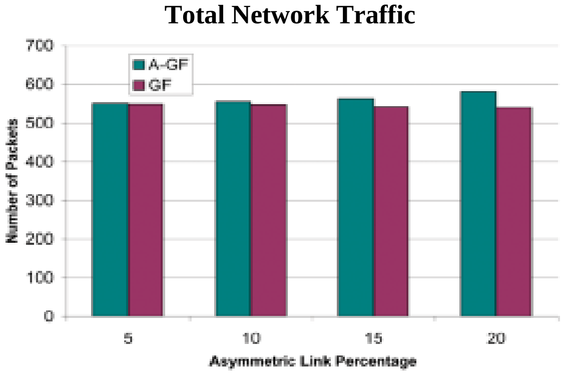


Figure1(f). Total Network Traffic

Seppo Virtanen also introduces that the A-GF, a location aware routing approach that actively exploits asymmetric links to increase the reliability and performance of ad-hoc routing. A-GF combines the two metrics stability and minimum latency while making routing decision.

K Pradeepa, Regis W Anne et.[9] Al. introduces that the clustering techniques in that the Sensors have become a very trendy research area during the last few years covering a wide range of applications such as habitat monitoring, military surveillance, information collecting etc. . . Sensors used for these purposes needs to be deployed very densely and in a random fashion. They should be able to operate without human intervention. Clustering is a technique employed to increase the various capabilities of a sensor network.

Boungju Jeon, Byeongkwan Kang et. al . High Event Density Area Centered Clustering based Routing for this they developed the WSN battrery powered device. They designed and implemented HEDACR to alleviate two WSN constraints. HEDACR forms a high density tree based cluster centered at the area with many sensors detecting events occurrence. HEDACR forms the multi-hop short distance routing path using a high density tree based cluster. They experimented with r proposed HEDACR and compared it with LEACH using one-hop data transmission. They also checked the sensor battery depletion time. The network lifetime of HEDACR is longer than the network lifetime of LEACH. HEDACR enables all sensors to participate in data transmission using the multi-hop short distance data transmission. Therefore, HEDACR diffuses energy consumption for data transmission and extends network lifetime [10].

III. METHODOLOGY

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Many data transmission protocols for WSN including the cluster based are vulnerable to number of security attacks. In cluster based protocols since the data aggregation and routing of data depends on CH.so the attacks to the CH can cause serious damage to the network. If an attacker manages to turn into a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, thus disrupting the network. On the other hand, the attacker may intend to inject bogus sensing data into the network, especially to pretend as leaf nodes sending bogus information towards the CHs.

Secure data transmission is a critical issue for wireless sensor networks (WSNs).Proposed two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/ offline digital signature (IBOOS) scheme, respectively. The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.

ID-based encryption (or identity-based encryption (IBE)) is an important primitive of ID-based cryptography. As such it is a type of public-key encryptionin which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This can use the text-value of the name or domain name as a key or the physical IP address it translates to.The first implementation of an email-address based PKI was developed by Adi Shamir in 1984, which allowed users to verify digital signatures using only public information such as the user's identifier.ID-based encryption was proposed by Adi Shamir in 1984 He was however only able to give an instantiation of identity-based signatures. Identity-based encryption remained an open problem for many years.

One of the major advantages of any identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. This can take place because this system assumes that, once issued, keys are always valid (as this basic system lacks a method of key revocation). The majority of derivatives of this system which have key revocation lose this advantage. Moreover, as public keys are derived from identifiers, IBE eliminates the need for a public key distribution infrastructure. The authenticity of the public keys is guaranteed implicitly as long as the transport of the private keys to the corresponding user is kept secure (Authenticity, Integrity, Confidentiality). Apart from these aspects, IBE offers interesting features emanating from the possibility to encode additional information into the identifier. For instance, a sender might specify an expiration date for a message. He appends this timestamp to the actual recipient's identity (possibly using some binary format like X.509). When the receiver contacts the PKG to retrieve the private key for this public key, the PKG can evaluate the identifier and decline the extraction if the expiration date has passed. Generally, embedding data in the ID corresponds to opening an additional channel between sender and PKG with authenticity guaranteed through the dependency of the private key on the identifier.

Secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based crypto-systems. Secure communication in SET-IBS relies on the ID-based cryptography, in which user public keys are their ID information. Thus users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.

Apply the symmetric key management for security, which suffers from a so-called orphan node problem. This problem occurs when a node does not share a pair wise key with others in its preloaded key ring. Furthermore, the orphan node problem reduces the possibility of a node joining with a CH, when the number of alive nodes owning pair wise keys decreases after a long-

SET-IBOOS is proposed in order to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. Both SET-IBS and SETIBOOS solve the orphan node problem in the secure data transmission with a symmetric key management.

The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols, respectively, for CWSNs, SET-IBS, and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks.

SET-IBS and SETIBOOS are efficient in communication and applying the IDbased cryptosystem, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management.With respect to both computation and communication costs, we pointed out the merits that using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

DISADVANTAGES:

- Difficult to keep multiple interior routers which configured correctly
- Complexity is high in packet filters.
- Energy consumption is high compared with the proposed system.
- Apply the symmetric key management for security, which suffers from a so-called orphan node problem. This problem occurs when a node does not share a pair wise key with others in its preloaded key ring.

In the Proposed system clustering and digital signature scheme is implemented for providing energy aware secure multipath routing.

Our contribution consists in reducing the control energy for cluster formation by keeping each selected cluster head for more than one transmission round. The proposed algorithm, called Clustering Technique for Wireless Sensor Net-works (CTRWSN) is a self-organizing, dynamic clustering method that divides dynamically, the network on a number of a priori fixed clusters. Each cluster has one cluster-head

Proposed uses a cluster head rotation in order to balance the transmission energy cost over the network nodes, because the cluster head role is energy expansive. That permits to grant approximately, the same lifetime until the battery energy depletion. So, in every transmission round, some new nodes play concurrence to be elected as cluster head. Each node selected, has to advertise its status to its neighbor nodes, to know the nodes which will belong to its cluster and to schedule the TDMA intervals.

Once the clusters are established, the nodes transmit their data messages towards the cluster-head. Within the cluster, the communication uses TDMA, as de-scribed in the set up phase. When the cluster-head receives all the nodes data, it performs its compression, to form a new message that sent to the base station.

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bit string: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

A digital signature scheme typically consists of three algorithms: A key generation algorithm that selects a private keyuniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. A signing algorithm that, given a message and a private key, produces a signature, A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of message to attach a code that act as a signature. It is formed by taking the hash of message and encrypting the message with creator's private key.

Network lifetime is an inevitable consideration in WSNs, because sensor nodes are constrained in power supply, processing capability and transmission bandwidth, especially for applications of harsh environments. Usually it is indispensable to minimize the energy consumption for intra-cluster communication by CHs which are richer in resources than ONs. Besides, sensor nodes that are close to most of the sensor nodes in the clusters should be prone to be CHs. Additionally, the aim of energy-aware idea is to select those routes that are expected to prolong the network lifetime in inter-cluster communications, and the routes composed of nodes with higher energy resources should be preferred.In order to increase the network life time we propose two secure and efficient data transmission protocol

Modern design of wireless devices requires the designers to have a special focus on power consumption to prolong the battery life of the final system.

The designer therefore needs power consumption information very early in the process to be able to decide on system parameters, design methods, communication protocols, and functionality restrictions. This is done by running simulations of the system to be developed and performing design space exploration.

However, there is a tradeoff between speed and accuracy of simulation, s this proposed system to save energy and improve the network lifetime. In the first phase, Networks are formed with the given range of the sensors. Nodes are grouped automatically depends upon their radio waves. Then in learning phase,learning automata is a machine that can do finite actions. Each selected action is evaluated by a possibilistic environment. Evaluation results are given to automata through positive and negative signals and automata uses these results to choose the next action. The ultimate goal is that automata can learn to choose the best among all. Here variable structure learning autometa algorithm is used for select the reliable and optimum route.

Then each node has learning automata with action number equal to number of paths from that node to destination. The protocol uses this to select appropriate path in order to balance energy usage. And in the proposed system implement two Secure and Efficient data Transmission protocols for CWSNs, called DSI and DSOO respectively. The key idea of both DSI and DSOO is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.

In the proposed protocols, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem. Finally that data transmission and analysis phase, in which the Proposed system uses the Homomorphic encryption for encrypting the data packet and uses hash functions for identifying the varying length and digital signature scheme for authentication. If the authentication is successful then it sends data packet through the Reliable routing path. Proposed a new protocol scheme DSI is also analyzed for security metrics. Various aspects of data transmission in wireless sensors are analyzed .In Learning Phase, rule based learning is analyzed for selecting reliable route and its performance metric is compared with the existing system. Proposed a new protocol scheme DSI is also analyzed for security metricfinally comparative analysis is made for security, energy-efficiency, and performance.

ADVANTAGES:

- Better Confidentiality - Protection from unauthorized persons
- Integrity - consistency of data
- Availability - ensuring access to legitimate users
- Energy-Efficient – less power consumption in order to increase network lifetime.

IV. CONCLUSIONS

Proposed a simple, secured and energy-aware protocol for intrusion detection in WSN. This system proposed two secure and efficient data transmission (SET) protocols for CWSNs, called DSI and DSIOO, by using the identity-based digital signature (IBS) scheme and the identity-based online/ offline digital signature (IBOOS) scheme, respectively. Proposed system is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.

To obtain the energy aware system clustering is implemented and cluster heads are elected depends upon the less energy consumption among the group of nodes within the communication range. After cluster head election the nodes are communicated via Cluster Head.

Finally comparative analysis is made for security, energy-efficiency, and performance. Simulation results show that energy-aware, secured data transmission with high level of performance achieved in this system.

REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[3] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.

[5] A. Manjeshwar, Q.-A.Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[6] S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.

[7] K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.

[8] L.B. Oliveira et al., "SecLEACH-On the Security of ClusteredSensor Networks," Signal Processing, vol. 87, pp. 2882-2895,2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and PerformanceAnalysis of a Secure Clustering Protocol for Sensor Networks,"Proc. IEEE Sixth Int'l Symp. Network Computing and Applications(NCA), pp. 145-152, 2007.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networkingand Mobile Computing (WiCOM), pp. 1-5, 2008.