Asian Journal of Information Technology 15 (4): 651-660, 2016
ISSN: 1682-3915

Hybrid Transmission Technique with Security in Heterogeneous Wireless Sensor Networks

[1]B. Elizabeth Caroline and [2]R.J. Kavitha
[1]Department of ECE, Ifet College of Engineering, Villupuram, India
[2]University College of Engineering, Panruti (A Consituent College of Anna University), 607106, Panruti, India

Abstract: Heterogeneous Wireless Sensor Network (HWSN) consists of sensor nodes with different ability such as different computing power and sensing range. The networks have a wide range of applications and they are prone to security threats and they do have a wide range of applications like military, environmental monitoring, health care, etc., traditional network security methods are not up to the mark due to limited resources. In this study, the energy efficient and security based Hybrid Transmission Technique with Security (HTTS) is proposed for HWSN to solve above issues. Initially, the clusters are created by using the formation of sensor nodes, which are have a Cluster-Head (CH) that are used to performs data aggregation in the cluster's sensor nodes then the aggregated data transmitting from multiple hops to the base station and this process reduces the bandwidth by eliminating the redundant data in a cluster. Then the energy efficient protocol called Hybrid Transmission Protocol (HTP) proposed for reduced the issues of limited power on mobile nodes. Second, the performance of a Cooperative Modulation Diversity (CMD) technique is evaluated. Finally, a key distribution scheme based on random key pre-distribution proposed for heterogeneous sensor networks to achieve better security and performance.

Key words: Heterogeneous Wireless Sensor Network (HWSN), Hybrid Transmission Technique with Security (HTTS), Cluster-Head (CH), Hybrid Transmission Protocol (HTP), Cooperative Modulation Diversity (CMD)

INTRODUCTION

Wireless Sensor Networks (WSN) consists of spatially distributed autonomous sensors and frames the sensor nodes for communication between each other. Sensors of different types have been used to monitor physical or environmental conditions such as temperature, sound, pressure, etc. and to cooperatively pass their data to a main location through the network (Boukerche *et al*., 2009; Akyildiz and Vuran, 2010). The development of wireless sensor networks was made by many potential applications such as battlefield surveillance in military field, industrial process monitoring and control in many industries, machine health monitoring, and so on (Akyildiz *et al*., 2002). An important problem in a wireless sensor network is the topology control. The necessity of topology control is to extend the network lifetime and to reduce power consumption (Li *et al*., 2008). Some other problems created are time synchronization, sensor transmission range, sensor location information, fault model in the network. To solve the above problems the clustering algorithms are used.

Clustered wireless sensor networks can be divided into two categories: homogeneous and heterogeneous networks. In homogeneous networks, all the sensor nodes are identical, i.e., hardware complexity, functionality and battery energy are identical. Heterogeneous WSN can be implemented using either staged architecture or by using hierarchical architecture. In staged architecture, nodes are arrange in series whereas in hierarchical nodes are arranged as a trees (Kavitha and Elizabeth 2015a). However, in heterogeneous networks, different types of nodes with different capabilities such as different functionality and different battery energy are used (Duarte-Melo and Liu, 2002).

By the use of many diversity techniques, the wireless communication channel faces many challenges such as signal fading which causes harmful effects in the network. They can be mitigated with the help of diversity techniques such as temporal, frequency and spatial diversity (Liu, *et al*., 2005; Lopes *et al*., 2006). The spatial diversity utilizes multiple antennas characteristically separated by a distance that reduces autocorrelation within the signal. There are many limitations such as use

Corresponding Author: Elizabeth Caroline, Department of ECE, Ifet College of Engineering, Villupuram, India

of multiple antennas in a single terminal is impractical, limitations in physical dimensions, high complexit and increase in power consumption. So, the proposed approach is going to use the cooperative modulation diversity technique (Sendonaris *et al*., 2003).

The network security is a main research in heterogeneous WSN. The confidentiality, integrity and authenticity of the data collected are the main issues in sensor network security. Wireless nature of the network along with the lack of computational ability of sensor nodes poses many challenges in the implementation of security protocol for WSN. The RSA-1024 and AES cryptographic standards are widely used in secure internet transactions. But, the computational cost of these schemes is not feasible over sensors nodes. Elliptic curve cryptography is proved to be the most suitable asymmetric key technique for WSN because of small key size (160 bit) with equivalent security (Hankerson *et al*., 2004). Effective applicability of these cryptographic schemes in the network depends on the key management technique used. Key management technique is the backbone of any network security scheme. Secured channel for data transmission in a WSN is provided by key establishment protocol.

In heterogeneous WSN, asymmetric key cryptography technique of ECC used. They contain a small number of powerful, High-Energy Sensor nodes (HES) and a large number of Low-Energy Sensor nodes (LES) (Zhang and Pengfei, 2014; Rahman and Sampalli, 2012). But, ECC is unsuitable for most sensor architectures due to high power consumption and increased code storage requirements. To avoid these problems hybrid key management has been developed to perform key management which uses the combination of both symmetric and asymmetric key cryptography in HSN (heterogeneous sensor networks). It achieves significant scalability (Kausar *et al*., 2008) and security (Huang *et al*., 2011).

In this study, initially the HTP (Kavitha and Caroline, 2015a) routing algorithm is presented and introduced a new border cluster between the cluster-heads and the sink in the network will minimize energy consumption in order to extend the network lifetime and achieve energy efficiency. Then CMD (Kavitha and Caroline, 2015b) evaluation is carried out impacts between the energy factor, lifetime, the channel Signal-to-Noise Ratio (SNR) and the packet loss rate is presented and results based on the maximum number of retransmissions, network size, packet length and initial energy by nodes are provided. A security process is a combination of symmetric and asymmetric keys were tried (hybrid) where the cluster head and BS use public key encryption based on ECC (Kavitha and Caroline, 2015c) while using symmetric key encryption between the adjacent nodes in the cluster. These all process achieved better performance and security in HWSN.

Literature review: Wireless sensor networks produce a large amount of data that needs to be processed, delivered and assessed according to the application objectives. The way these data are manipulated by the sensor nodes is a fundamental issue. Information fusion arises as a response to process data gathered by sensor nodes and benefits from their processing capability. In a survey of the key aspect of the algorithm is to reduce the number of messages for setting up a routing tree, high aggregation rate and reliable data aggregation and transmission (Nakamura *et al*., 2007). In the modified DRINA algorithm, cluster head is responsible for aggregating the data of all its neighbor nodes and transmit it through the shortest and energy efficient, reliable path, which results increase in throughput, lifetime, PDR and control overhead.

Saini and Sharina (2013) proposed an energy efficient cluster head election scheme for heterogeneous WSNs. The author have adjusted the value of the threshold, according to which a node decide to become a cluster head or not, based on the ratio of residual energy and average energy of that round in respect to the optimum number of cluster heads. Two level and three levels of heterogeneous nodes are considered in the algorithm and after that a general solution for multilevel heterogeneity is proposed. It requires the average network energy for cluster head selection, which is more energy consumable.

Javaid *et al*. (2013) and Qureshi *et al* (2013) proposed new protocol Enhanced Distributed Energy Efficient Clustering (EDEEC) for three types of nodes in prolonging the lifetime and stability of the network. Hence, it increases the heterogeneity and energy level of the network. Simulation results show that EDEEC performs better than SEP with more stability and effective messages.

Javaid *et al*. (2013) proposed BEENISH (Balanced Energy Efficient Network Integrated Super Heterogeneous) protocol. It assumes WSN containing four energy levels of nodes. Here, Cluster Heads (CHs) are elected on the bases of residual energy level of nodes. Simulation results show that it performs better than existing clustering protocols in heterogeneous WSNs. Our protocol achieves longer stability, lifetime and more effective messages than Distributed Energy Efficient Clustering (DEEC), Developed DEEC (DDEEC) and Enhanced DEEC (EDEEC).

Tao *et al*. (2012) presented overview of cooperative communications. It fundamentally, change the abstraction

of a wireless link and offer significant potential advantages for wireless communication networks. This article visits cooperative techniques, such as relay, Distributed Antennas Systems (DAS), multicell coordination, group cell, Coordinated Multiple Point transmission and reception (CoMP), those turn the traditional cellular system into a cooperative system.

Nosratinia *et al.* (2004) proposed cooperative communication that enables single antenna mobiles in a multi-user environment to share their antennas and generate a virtual multiple-antenna transmitter that allows them to achieve transmit diversity. Zhang and Zhang (2008) investigated the joint problem of routing selection in network layer and contention avoidance among multiple links in MAC layer for multi-hop wireless networks in a cooperative communication aware network. Several important concepts including virtual node, virtual link and virtual link based contention graph are introduced. Basing on those concepts, an optimal cooperative routing is achieved and a distributed routing scheme is proposed after some practical approximations.

Khandani *et al.* (2007) studied the problem of transmission-side diversity and routing in a static wireless network. It is assumed that each node in the network is equipped with a single omnidirectional antenna and that multiple nodes are allowed to coordinate their transmissions in order to obtain energy savings. Analytical results derived for achievable energy savings for both line and grid network topologies. It is shown that the energy savings of and are achievable in line and grid networks with a large number of nodes, respectively. Then, develop a dynamic-programming-based algorithm for finding the optimal route in an arbitrary network as well as suboptimal algorithms with polynomial complexity.

Du *et al.* (2007) present an effective key management schemes-the Asymmetric Predistribution (AP) scheme for HSNs. The powerful H-sensors are utilized to provide simple, efficient and effective key set up schemes for L-sensors. Although, tamper-resistant hardware is too expensive for L-sensors, it is reasonable to assume that powerful H-sensors are equipped with this technology. The basic idea of the AP key management scheme is to pre-load a large number of keys in each H-sensor while only pre-loads a small number of keys in each L-sensor. A H-sensor has much larger storage space than an L-sensor and the keys pre-loaded in an H-sensor are protected by the tamper-resistant hardware.

Du *et al.* (2009) propose a routing-driven key management scheme, which only establishes shared keys for neighbor sensors that communicate with each other. Elliptic curve cryptography is utilized to further increase the efficiency of the key management scheme. The performance evaluation and security analysis show that the routing-driven key management scheme provides better security with significant reductions on communication overhead, storage space and energy consumption than some existing sensor key management schemes.

Traynor *et al.* (2006) also assume that there are nodes in the network that are more powerful and more secure than others and these more powerful nodes are also in tamper proof boxes or well guarded. A node that has limited memory and processing power is identified as L1 and a node that have more memory and more processing power is identified as L2. L2 nodes act as head nodes for the L1 nodes and have the responsibility of routing packets throughout the network. These L2 nodes have access to gateway servers which are connected to a wired network.

MATERIALS AND METHODS

In this proposed system, initially the HTP routing algorithm is presented and introduced a new border cluster between the cluster-heads and the sink in the network will minimize energy consumption in order to extend the network lifetime and achieve energy efficiency. Then CMD evaluation is carried out impacts between the energy factor, lifetime, the channel Signal-to-Noise Ratio (SNR) and the packet loss rate is presented and results based on the maximum number of retransmissions, network size, packet length and initial energy by nodes are provided. A security process is a combination of symmetric and asymmetric keys were tried (hybrid) where the cluster head and BS use public key encryption based on ECC while using symmetric key encryption between the adjacent nodes in the cluster.

System and network model: To meet the demands of efficient environmental monitoring proposed HTTS model designed with both different initial energies and monitored nodes. The basic assumptions of networks model: the networks is located in a $M \times M^2$ area, N sensor nodes are randomly distributed within the networks, nodes are slightly mobile and base station is located in the middle of the area. The networks perform the task of environmental monitoring and sensor nodes monitor a variety of nodes.

Network model: The network model is illustrated in Fig. 1. It consists of two types of sensor nodes. The large number of Low-Energy Sensors (LES) that has a lower

energy, limited computation, Small number of High-Energy Sensors (HES) which have a great energy, high computation, high communication and storage capacity than LES. There are powerful HES serving as cluster heads in this method. Assume that the Base Station (BS) is trusted and has sufficient energy. All of the nodes are static and they know their own location information and HES are uniformly deployed in the monitoring area. Due to energy constraints, LES are not equipped with tamper resistant hardware. HES are equipped with tamper resistant hardware communication and storage capacity.

Hybrid Transmission Protocol (HTP): A Hybrid transmission protocol proposed for the heterogeneous environment. In a multi-hop communication, the failure of one relay node can lead to the disconnection of a number of nodes from the base station. To ensure energy effective and self-adaptive operations of sensor networks, the design takes into account the Energy-level (E) and the distance to cluster-heads D in the network as the key parameters. In order to achieve an acceptable Signal-to-Noise Ratio (SNR) in transmitting an L-bit message over a distance d, the energy E_{TX} disbursed by the radio is given by:

$$E_{TX}(L,d)=\begin{cases}L\times E_{elec}+L\times\varepsilon_{fs}\times d^2, d<d_0\\ L\times E_{elec}+L\times\varepsilon_{mp}\times d^2, d\geq d_0\end{cases} \quad (1)$$

$$d_0=\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} \quad (2)$$

Where

E_{elec} = The energy dissoluted per bit to operate the transmitter or receiver circuit

ε_{fs} and ε_{mp} = Depends on the transmitter amplifier model

d = The distance between the sender and the receiver

Besides, the radio expends an amount of energy E_{RX} is receiving an L-bit message as follows:

$$E_{RX}(L)=L\times E_{elec} \quad (3)$$

In HTP, the distance metric is considered during the cluster construction phase when nodes join the nearest cluster-head, the HTP of which to join being made on a node-by-node basis. This feature means that the algorithm is less centralized and thus, has better scalability properties than algorithms that require extensive state information during cluster construction. It considers a two-tier model and a wireless sensor network consisting of a base station and n sensors. It is assumed that the initial energy of the nodes in the network is known.

Cooperative Modulation Diversity (CMD): Cooperative modulation diversity has the prospective to be used in wireless sensor networks. The CMD utilizes diversity enhancement in a system when independent channel fading affects each and every element of the transferred signal. It provides higher throughput and robustness to channel variations for both the transmitting and relaying mobiles. The concept of the subsidiary cluster head was provided to support the operation of multi hooping in wireless sensor networks which is raised in adaptive manner and it is needed only, if transmission errors occur. Basis cluster head can be performed in two stages during next hop transmission, i.e., transmission and retransmission stage.

Transmission stage: On the transmission stage, basis cluster-head transfers its clustered information to another nearest neighbor cluster-head and the next hop in the direction finding process towards the base station. By the transmission nature of the wireless channel, the subsidiary cluster head accepts the transmitted packet from the basis cluster-head. The lasting cluster sensor nodes save energy by triggering the snooze mode. The conservative QPSK modulation method is used for transmission of packets. The equation which representing modulated signal is given by:

$$m(t)=A_c\sum_{n=-\infty}^{\infty}x_n p(t-nTs)\cos(2\pi f_c t)+A_c\sum_{n=-\infty}^{\infty}y_n p(t-nTs)\sin(2\pi f_c t) \quad (4)$$

In which X_n, $Y_n=\pm 1$ with equal probability:

$$P(t)=\begin{cases}1, 0\leq T_s\\ 0, \text{elsewhere}\end{cases} \quad (5)$$

For carrier amplitude, A_c and a carrier frequency, F_c. A CRC is attached to the transmitted packet and identified by the receiver (either nearest cluster-head or the subsidiary cluster-head or the base station). An acknowledgement is received by the basis cluster-head when the packet is correctly received by the receiver. The basis cluster-head starts to transmit new packets and the earlier process is repetitive. Or else, retransmission stage begins.

Retransmission stage: Retransmission of packets takes place by the use of cooperative modulation diversity

when the subsidiary cluster-head receives the packet correctly in cooperation with the basis cluster-head. Or else, the subsidiary cluster-head saves energy by triggering snooze mode by using QPSK transmission another time. The retransmissions persist till the packet is effectively delivered or the number of retransmissions surpasses which is a predetermined parameter signifying the maximum number of retransmissions permitted per packet. The value depends upon the applications used in WSNs. Some kind of redundancy is introduced between the two quadrature channels when a QPSK pattern is rotated by a definite angle. Then, both the basis and subsidiary cluster-heads rotate the QPSK pattern by an angle Φ:

$$m(t) = A_c \sum_{n=-\infty}^{\infty} a_n p(t - nTs)\cos(2\pi f_c t) + A_c \sum_{n=-\infty}^{\infty} b_n p(t - nTs)\sin(2\pi f_c t) \quad (6)$$

In which $a_n = X_n \cos \Phi - y_n \sin\Phi$, $b_n = y_n \sin\Phi + y_n \cos \Phi$. Each component gets interleaved independently and quadrature component gets generated. The two components will be independent after deinterleaving so that the signal interleavers are selected. It can be understandable that the nodes engaged in the cooperative modulation transmission send merely half of the information from the total information separately. Up conversion of carrier frequency and an addition takes place between two components using the following equation:

$$m(t) = A_c \sum_{n=-\infty}^{\infty} a_n p(t - nT_s)\cos(2\pi f_c t) + A_c \sum_{n=-\infty}^{\infty} b_{n-k} p(t - nT_s)\sin(2\pi f_c t) \quad (7)$$

Channel model and decoding technique: Let us consider a communication channel which is a frequency non selective slowly fading channel with a multiplicative element that represents the effect of fading and an additive term that represents the Gaussian noise. The received signal is represented by:

$$r_s(t)\alpha_n(t)m(t) + n(t) \quad (8)$$

In which an is demonstrated as a zero-mean complex Gaussian process. The received signal (t) is converted to base band. The low pass signal is obtained in a single signaling interval which is given by:

$$r_s(t)\alpha_n e^{-j\theta}{}_n m_l(t) + Z_l(t), nTs \le t \le (n+1)T_s \quad (9)$$

In which (t) represents the complex white Gaussian noise, is the phase shift due to the channel fading, an is the fading amplitude considered to be constant over one symbol interval and ml (t) is a signal which corresponds to the equivalent low pass transmitted signal m (t). At the base station, received signal performs phase shift estimation and finally, the received vector after the demodulation is given by:

$$r_s = \alpha_n m_l(t) + Z_l \quad (10)$$

In which ml is the vector representation of the transmitted signal at time nTs and zl represents a complex vector where the elements in it are identical Gaussian random variables with mean value 0 and variance NO/2. After the deinter leaving process, the decoded vector at the base station is given by:

$$r_s = \alpha_n x_n + \mathrm{Re}\{Z_n\} + j[\alpha_n + kYn + \mathrm{lm}\{z_n\}] \quad (11)$$

which is handled by using symbol-by-symbol detection? The squared Euclidean distance between the received vector and each of the four vectors is computed by the demodulator and then chooses one which is nearest to rs.

Cryptographic technique for HSN: Recent researches have shown that using asymmetric key cryptography in Heterogeneous Sensor Networks (HSN) can improve network performance, such as connectivity, resilience, etc. Considering the pros and cons of symmetric key cryptography and asymmetric key cryptography, the paper proposes a Hybrid Key Management method (HKM) for heterogeneous wireless sensor network. In HKM, cluster heads and base stations use public key encryption method based on Elliptic Curve Cryptography (ECC) whereas symmetric encryption method between adjacent nodes in the cluster.

Preloading of key: The ECC method is used to generate the required pair of public and private keys for LES, HES and BS. The LES are assigned with a unique id and its public and private key with hash function. The HES are assigned with their public key and private key and also the public key of all LES, the public key of base station and hash function. The BS is preloaded with its own public and private keys and also with the public key of cluster head.

Deployment of cluster and establishing key: After sensor deployment clusters are formed in an HSN where HES

serve as cluster heads and form clusters around them. Each HES broadcasts 'm' message which includes the id and its location with a random delay. Each LES may receive a message coming from more than one HES then it chooses HES whose my message has the best signal strength. After that, each LES node sends its location information, including its id to its cluster head. It computes Message Authentication Code (MAC) over the message by using its Private Key and MAC is appended to message. The HES-Node can verify the MAC and then authenticate LES nodes identify, by using LES"s Public key and HES generates a certificate for LES"s Public key by using HES's Private key. The HES-Node determines the routing tree structure (i.e., parent-child relationship) in cluster and sends to all LES-nodes with the corresponding public key certificate to each LES. The public key certificates are signed by HES's private key and can be verified by every LES, since each LES is preloaded with HES's public key. A public key certificate proves the authenticity of a public key and further proves the identity of one LES to another LES. HES and BS have sufficient energy; they can communicate with each other by using signature encryption algorithm based on ECC.

Elliptic Curve Digital Signature algorithm allows verifying authenticity without compromising security. A curve on a graph using mathematical equations and a random point is chosen on that curve and consider that point is the origin. Then generate a random number, this is the private key by doing some magical mathematical equation using that random number and that "point of origin", we get a second point on the curve, that's the public key. To sign a file, use this private key (the random number) with a hash of the file (a unique number to represent the file) into a magical equation and that gives signature. To confirm the authenticity we have to divide signature into two parts using the public key. One part of the equation is put into a mathematical formulation. If we are able to get back another part of the mathematical formulation using our private key then it is clear that security is secure. There is no way to know the private key or to create a signature using only the public key.

The algorithm used to establish a shared key between the cluster heads and the nodes in its cluster is ECDH. The Elliptic Curve Diffie Hellman (ECDH) is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public-private key pair to establish a shared secret over an insecure channel. This shared secret may be directly used as a key or to derive another key which can then be used to encrypt subsequent communications using a symmetric key cipher. Here common key is generated using point P for

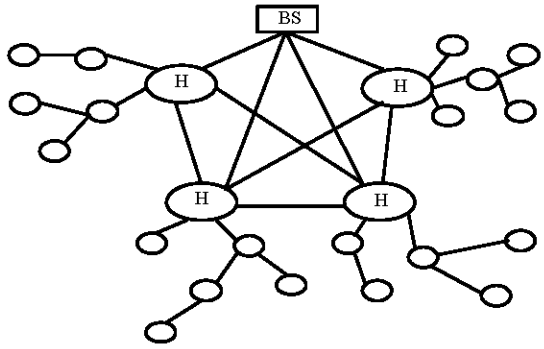

Fig. 1: Network model

sensors as follows, shared key of HES:

$$KH_jL_i = p^rH_j \times p^mL_i = p^rH_j \times p^rL_i \times p \quad (12)$$

Shared key of LES:

$$KH_jL_i = p^rL_i \times p^mH_j = p^rL_i \times p^rH_j \times p \quad (13)$$

Where:

P = The point multiplication factor of the elliptic curve
P^rH_j = The private key of HES
P^rL_j = The private key of LES
P^mL_i = The public key of LES
P^mH_j = The public key of HES

The limited energy of LES makes it unfit for public key encryption so that symmetric session key is established between adjacent LES using a one way hash function.

Key withdrawal: When the LES are captured and become compromised nodes then their keys have to be revoked. Using the intrusion detection method we detect the compromised nodes within the network. Figure 1 HES broadcast a warning about intrusion to its LES. In turn, LES checks whether it communicates by the intruded node, if so it terminates the connection.

Key renewal: Due to low energy consumption in the symmetric key cryptography, its security level is lower than public key cryptography. So, it is necessary to update the shared keys between LES regularly to prevent them from enemy being hacked. This is known as key renewing. The energy consumption of key updating is low.

RESULTS AND DISCUSSION

In this study, the experimental results of the proposed Hybrid Transmission Technique with Security (HTTS) discussed and evaluated. The HTTS performance is compared with existing Low Energy Adaptive Clustering Hierarchy (LEACH) (Sujee and Kannammal, 2015) protocol. For the performance evaluation, here this work used the NS2 simulator. Simulations specification is used in this work are described in Table 1.

Performance evaluation: This research considered the following important performance metrics for the evaluation by simulation.

Energy consumption: Figure 2 illustrates the relationship between the energy consumption on communications and the number of nodes. The HTTS has a less power computation than LEACH. Nonetheless, when consider the (energy) consumption incurred by both computation and communication, HTSS is still relatively efficient when number of nodes is large.

Delivery Ratio (DR): The ratio between the numbers of messages correctly received by the sink to the number of messages generated by all sensor nodes:

$$DR = \frac{\sum \text{Number of messages recieve}}{\sum \text{Number of messages send}} \times 100 \qquad (14)$$

The delivery ratio is described in Fig. 3, it is simply the ratio of the number of delivered and transmitted message to the destination node. It is usually, portrays the state of message sent to the destination node. Through, the use of proposed method HTTS is attained, implying HTTS performs much better by attaining the best delivery ratio in comparison with existing LEACH method.

Throughput (TP): Throughput is defined as the total number of messages delivered over the total simulation time. Mathematically, it can be defined as:

$$Tp = N/1000 \qquad (15)$$

where is the number of bits received successfully by all destinations. Figure 4 shows, the comparison result of throughput from the proposed HTTS method and the existing LEACH method. It is noted that the proposed HTTS attains higher throughput when compared with LEACH.

Table 1: Simulations specification

Network parameters	Range
Network area	100*100
BS location	(50,50)
Number of nodes	100
E_0 (initial energy)	0.5J
Packet size	4000 bits
E_{elec}	50nJ/bit
$E_{TX} = E_{RX}$	50nJ/bit
E_{fs}	10pJ/bits/m^2
E_{MP}	0.0013pJ/bits/m^2

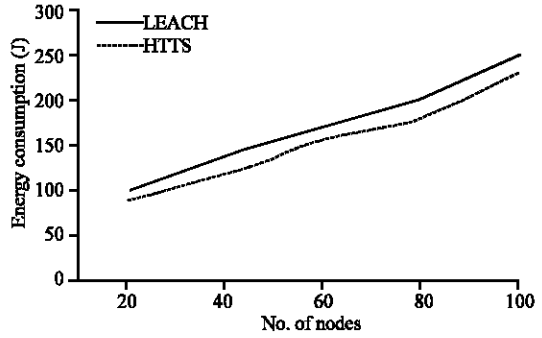

Fig. 2: Energy consumption vs No. of nodes

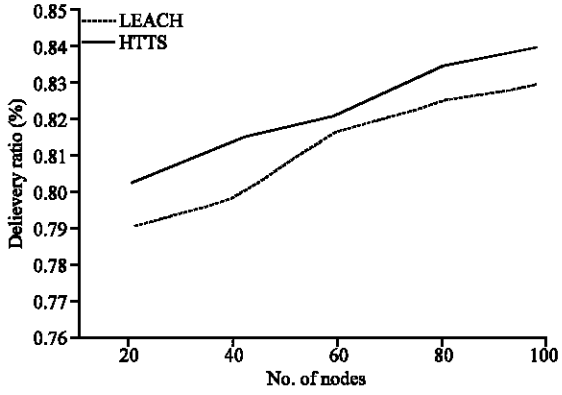

Fig. 3: Delivery ratio vs No. of nodes

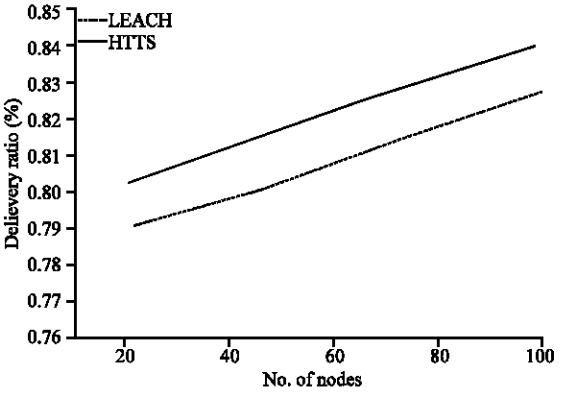

Fig. 4: Throughput vs No. of nodes

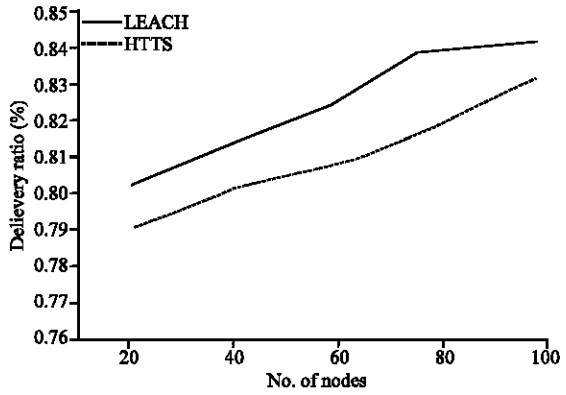

Fig. 5: EED vs No. of nodes

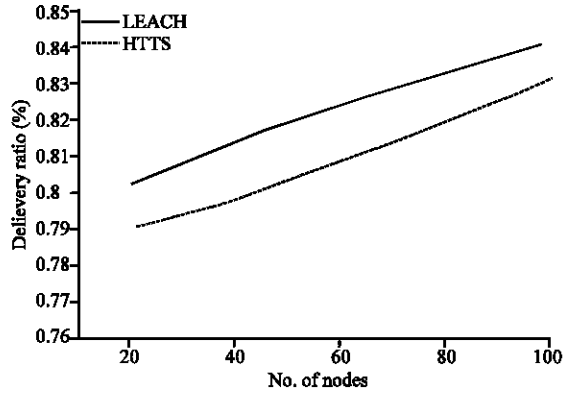

Fig. 6: Routing overhead vs No. of nodes

End-to-End Delay (EED): The end-to-end delay is calculated by obtaining time delay of a message between the source nodes to destination node:

$$EED = \Sigma \left(\frac{\text{Message reach time} - \text{Message send time}}{\Sigma \text{Number of connection}} \right) \quad (16)$$

Figure 5 compares the end-to-end delay between proposed HTTS with existing LEACH method. If the size of increased, the HTTS uses a active energy consumption mechanism to detect probable link breaks between the source and destination nodes and quickly apply an alternative path finding mechanism for message transfer. Moreover, when the no. of nodes is increased, the proposed method established a reduction in delay by than in existing methods.

Routing overhead: The total number of control messages transmitted during simulation. For messages sent over multiple hops, each transmission over one hop is counted as one transmission.

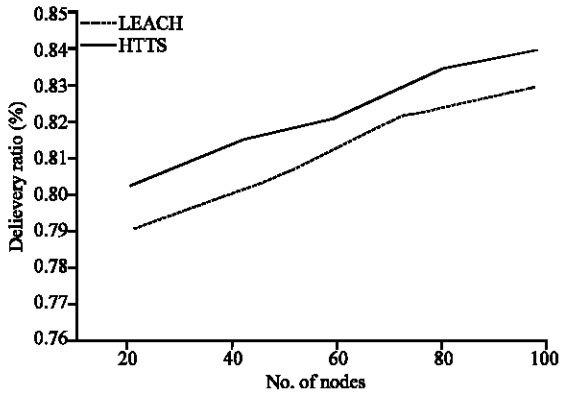

Fig. 7: Message size vs security level

Figure 6 compares the routing overhead between proposed HTTS and existing LEACH method. When the size of the network is 80 nodes, the routing overhead of proposed approach is considerably lesser than that of existing approaches. When the size of the network is increased to 100 nodes, the routing overhead of proposed HTTS was lesser than existing LEACH method. Moreover, with the size of the network was increased to above 100 nodes, the HTTS demonstrated less routing overhead in control messages than existing methods.

Security level: Figure 7 shows the message size has a linear relationship with the security level is observed. The security level of proposed HTTS was higher security than LEACH method, with the size of the network was increased means, the HTTS demonstrated higher security in control messages than existing LEACH method.

CONCLUSION

In this study, a new Hybrid Transmission Technique with Security (HTTS) proposed for heterogeneous wireless sensor network. This proposed cluster has Cluster-Head (CH) that performs data aggregation by the sensor nodes and further transmitting them by multiple hops to the base station and reduces the bandwidth by eliminating the redundant data in a cluster. Then the three proposed techniques are processed such as:

- Hybrid Transmission Protocol (HTP)
- Then, evaluates the performance of a Cooperative Modulation Diversity (CMD) technique
- Proposed a key distribution scheme based on random key pre-distribution for heterogeneous sensor networks to achieve better security

This study examined energy optimization methods, clustering schemes that have been employed in

heterogeneous WSNs to improve the energy-efficiency in a hierarchically clustered deployment. By using CMD, Packet loss rate diminution occurs by increasing SNR value where less energy consumption takes place and also proposed network lifetime increases. The Cryptographic key management method can provide better security, scalability than other previous methods.

REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Networks, 38: 393-422.

Akyildiz, I.F., and M.C. Vuran, 2010. Wireless Sensor Networks. John Wiley and Sons, New York.

Boukerche, A., E. Nakamura and A. Loureiro, 2009. Algorithms for Wireless Sensor Networks: Present and Future. In: Algorithms and Protocols for Wireless Sensor Networks, Boukerche, A. (Ed.). John Wiley and Sons, New York pp: 1-19.

Du, X., Y. Xiao and H. Chen, 2009. A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks. IEEE Trans. Wireless Commun., 8: 1223-1229.

Du, X., Y. Xiao, M. Guizani and H.H. Chen, 2007. An effective key management scheme for heterogeneous sensor networks. Ad Hoc Networks, 5: 24-34.

Duarte-Melo, E.J. and M. Liu, 2002. Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks. Proceedings of the IEEE Global Telecommunications Conference, November 17-21, 2002, Taipei, Taiwan, pp: 21-25.

Hankerson, D., S. Vanstone and A. Menezes, 2004. Guide to Elliptic Curve Cryptography. Springer-Verlag, New York, ISBN-13: 9780387952734, Pages: 311.

Huang, J.Y., I.E. Liao and H.W. Tang, 2011. A forward authentication key management scheme for heterogeneous sensor networks. EURASIP J. Wireless Commun. Network., Vol. 6. 10.1155/2011/296704

Javaid, N., T.N. Qureshi, A.H. Khan, A. Iqbal, E. Akhtar and M. Ishfaq, 2013. EDDEEC: Enhanced developed distributed energy-efficient clustering for heterogeneous wireless sensor networks. Procedia Comput. Sci., 19: 914-919.

Kausar, F., S. Hussain, L.T. Yang and A. Masood, 2008. Scalable and efficient key management for heterogeneous sensor networks. J. Supercomput., 45: 44-65.

Kavitha, R.J. and B.E. Caroline, 2015. Hybrid cryptographic technique for heterogeneous wireless sensor networks. Proceedings of the IEEE International Conference on Communications and Signal Processing, April 2-4, 2015, Melmaruvathur, pp: 1016-1020.

Kavitha, R.J. and B.E. Caroline, 2015. Proxum: An energy efficient and privacy-aware data aggregation in heterogeneous wireless sensor networks. Adv. Natural Applied Sci., 9: 316-322.

Kavitha, R.J. and B.E. Caroline, 2015. Subsidiary cluster head with cooperative modulation diversity applied to heterogeneous wireless sensor networks. Proceedings of the IEEE International Conference on Communications and Signal Processing, April 2-4, 2015, Melmaruvathur, pp: 1281-1285.

Khandani, A.E., J. Abounadi, E. Modiano and L. Zheng, 2007. Cooperative routing in static wireless networks. IEEE Trans. Commun., 55: 2185-2192.

Li, X., Y. Mao and Y. Liang, 2008. A survey on topology control in wireless sensor networks. Proceedings of the 10th International Conference on Control, Automation, Robotics and Vision, December 17-20, 2008, Hanoi, pp: 251-255.

Liu, W., X. Li and M. Chen, 2005. Energy efficiency of MIMO transmissions in wireless sensor networks with diversity and multiplexing gains. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Vol. 4, March 18-23, 2005, IEEE., pp: 897-900.

Lopes, W.T.A., F. Madeiro, J.F. Galdino and M.S. Alencar, 2006. Impact of the estimation errors and doppler effect on the modulation diversity technique. Proceedings of the IEEE Vehicular Technology Conference, September 25-28, 2006, Montreal, Que, pp: 1-5.

Nakamura, E.F., A.F. Loureiro and A.C. Frery, 2007. Information fusion for wireless sensor networks: Methods, models and classifications. ACM Comput. Surv., Vol. 39 10.1145/1267070.1267073

Nosratinia, A., T.E. Hunter and T.A. Hedaya, 2004. Cooperative communication in wireless networks. J. Commun. Magazine, 42: 74-80.

Qureshi, T.N., N. Javaid, A.H. Khan, A. Iqbal, E. Akhtar and M. Ishfaq, 2013. BEENISH: Balanced Energy Efficient Network Integrated Super Heterogeneous protocol for wireless sensor networks. Procedia Comput. Sci., 19: 920-925.

Rahman, M. and S. Sampalli, 2012. A hybrid key management protocol for wireless sensor networks. Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, June 25-27, 2012, Liverpool, pp: 769-776.

Saini, P. and A.K. Sharma, 2010. Energy efficient scheme for clustering protocol prolonging the lifetime of heterogeneous wireless sensor networks. Int. J. Comput. Applic., 6: 30-36.

Sendonaris, A., E. Erkip and B. Aazhang, 2003. User cooperation diversity. Part I. System description. IEEE Trans. Commun., 51: 1927-1938.

Tao, X., X. Xu and Q. Cui, 2012. An overview of cooperative communications. IEEE Commun. Mag., 50: 65-71.

Traynor, P., H. Choi, G. Cao, S. Zhu and T. Porta, 2006. Establishing pair-wise keys in heterogeneous sensor networks. Proceedings of the 25th IEEE International Conference on Computer Communications, April 23-29, 2006, Barcelona, Spain, pp: 1-12.

Zhang, J. and Q. Zhang, 2008. Cooperative routing in multi-source multi-destination multi-hop wireless networks. Proceedings of the IEEE 27th Conference on Computer Communications, April 13-18, 2008, Phoenix, AZ., pp: 306-310.

Zhang, Y. and J. Pengfei, 2014. An efficient and hybrid key management for heterogeneous wireless sensor networks. Proceedings of the IEEE 26th Chinese Control and Decision Conference, May 31-June 2, 2014, Changsha, pp: 1881-1885.