International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Trust based Secure Routing using Cross layer for Heterogeneous Environment in WSN

Manisha R. Dhage, Srikanth Vemuru

Abstract: ***Many applications of Wireless Sensor Network which handles sensitive information like target tracking, surveillance and reconnaissance. Therefore, sensor nodes deployed in unprotected and open region should be vulnerable to attacks. Many of existing methods are defending against single layer attack and mechanism used for specific attack without considering other attacks. Literature focused on source or destination trustworthiness, not both. However, the problem with this existing method is that the solution for the Sybil attack does not defend against Jamming attack. Our proposed cross layer based trust estimation method provide defense against multiple attacks. In first part forwarding attacker node are detected by calculating trust by pulling multiple parameters from Network layers and MAC layer for forwarding node. In second part source attacker node is detected by utilizing MAC layer information that is a number of medium access per second for every node. In addition to this proposed method uses heterogeneous nodes which are suitable for real time application and cross layer method which improves energy efficiency.***

Keywords: ***Heterogeneous WSN, trust based security, cross-layering, clustering.***

I. INTRODUCTION

Wireless Sensor networks are more attractive to attacker because of its wireless nature. Due to limited resources like processing speed, battery power and memory, designing and applying security is very challenging task. To provide security cryptographic algorithm is one of the method but it gives problems due to message expansion of cipher text which consumes more energy, memory and bandwidth when it used in multi-hop network. This type of network suffers shorter lifetime and increased delay [1]. So, to provide security we could not use cryptographic algorithm. Due to all these reasons, alternative to traditional security method has been introduced and that is trust based system [2]. Cross layer method is giving good performance in wireless network by taking multiple system parameters from different layers. Comparative study given in literature showed that cross layer framework able to provide security to multiple layers and which improves energy efficiency also.

Many routing protocols, such as CBF [3], GPSR [4], and XLP [6] IGF used cross layer method and these protocols shows improvement in QoS and energy.

Our proposed trust based method using cross layer that secures wireless sensor network robustly. The system provides security to both source and destination by using information of different layers using cross layer method.

II. LITERATURE REVIEW

In Wireless sensor network research, the person who proposed routing protocol has not considered security for that routing protocol. They are just focusing on energy efficiency. In [6] author proposed energy efficient routing protocol (EERP) using A* algorithm. Proposed scheme improve network lifetime by using optimal path which is calculated based on high link quality, minimum hop counts, maximum residual energy of the next hop sensor node and buffer occupancy for forwarding packet but they have not provided security for that routing protocol. In [7] author proposed energy efficient clustering algorithm. They have focused on energy efficiency and not considered security. So there is need to design routing protocol which provide security also. In recent years many researchers worked on secured routing. We have also proposed energy efficient cross layer multihop routing protocol for heterogeneous WSN [8]; here we have focused on energy efficiency. That protocol is cluster based and we used multiple cross layer features to select cluster head. But again the same problem with this method is that we have not considered security of routing protocol.

So to provide security to energy efficient routing protocol many traditional methods are available like cryptography and authentication. But these methods provide security up to some extent because they cannot handle attacks of compromised node [9]. Once sensor node gets compromised, that node can attack from outside instructions. Key management is used for security and on adding it to routing the routing protocols, gives more problem like consumption of memory, bandwidth, and energy in multihop network due to cipher and decipher the text [2]. This type of network suffers, shorter lifetime, increased delay and in some cases zero delivery due to exhausted nodes.

Due to above discussed causes, methods using the trust are realized as a substitute to old security towards secure data routing in WSN. Hence, Trust based method enhances security by continuous scanning the node activities or behavior and then assessing the reliability of the nodes.

Manuscript published on January 30, 2020.
* Correspondence Author
Mrs Manisha R. Dhage*, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, 522502, Andhra Pradesh, India
Dr. Srikanth Vemuru, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, 522502, Andhra Pradesh, India

In compromised node detection, trust mechanism is easy and effective, a major work is done to improve and enhance communication among the nodes in the network [9].
In [10] four methods of trust estimation process are given and these are probability based, Fuzzy logic based, weighted based and Miscellaneous out of that Fuzzy logic method is more energy efficient.
Many trust mechanism are proposed for secure routing. In [9] paper they specified some issues and challenges. For instance watchdog mechanism which consumes more energy in transmission overhearing, watchdog mechanism do not distinguish among packet drop owing to collision ,channel condition or due to malicious node , proposed scheme for wormhole attach must consider energy factor in routing , proposed schemes are designed for single attack .
In [11] method they have used flat routing , which is not energy efficient where source node send recommendation request to search trusted node then it send route request , if that node is having route to endpoint they would send response to source node if not source node continue with same procedure . In [12] they have proposed energy efficient trust based clustering algorithm. Selection of Cluster head build on trust of member nodes and some other variables like degree of connectivity, waiting time and relative mobility nodes. They have used weighting based estimation, which attach weighting factors to above mentioned variables to verify whether the values are determined within allocated threshold. But, randomly selected weighting factors may disturb the result of the estimation and parameter combination.

III. PROPOSED METHODOLOGY

This section, a brief description is given for finding trusted forwarding node and trusted source node. Cluster based Routing protocol [8] used here is energy efficient. But in this routing algorithm security is not provided. So while selecting forwarding node that is cluster head, proposed trust based method is applied. In the second phase of proposed method, cluster head checks trustworthiness of cluster member. Trust assisted routing provides reliable and efficient routing paths without any selfish, faulty and malicious nodes. Proposed trust based secure routing using cross layer comprises of following two phases.

A. Cluster head Trustworthiness

In addition to energy efficient cluster head(CH) selection, proposed method finds the trustworthiness of to be cluster head. Cross layer method is used to find malicious behavior of node by using information fetched from multiple layers. Here nodes decide whether to become cluster head or not. Node which want to be cluster head, sends three values (remaining energy, nodes proximity with neighboring nodes, Link quality indicator) mentioned in [8] to the nodes in communication range. Then each node within range ask for different parameters from would be cluster head like ω, βop, Tr , d_{RTS} , E_{re} after a time period. The first and second parameter is used for local congestion control. The quality of connection, which depends on distribution, is denoted by ω CTS response time ω. The βop (buffer occupancy) second parameter ensures that the node does not experience any buffer overflow and hence, also prevents congestion. T is trust value of individual node based on direct observation [13], using watchdog mechanism. Node q calculates the trust value (Tpq) of a node p in its range as function (f) as shown in (2). The parameters monitored for a one-hop neighbor is shown in (3) and (4) which includes traffic statistics and traffic volume. To avoid more energy consumption in transmission overhearing of watchdog operation we can make that operation periodic.

Distance value d_{RTS} among the competing and the source node, which is again computed like [8] and last parameter is, E_{re}, which is remaining energy. All the parameters like ω, βop, Tr , d_{RTS} , E_{re}, are piggybacked with CTS and sent after a time period. Using all these parameters ID (Initiative Determination) is estimated which decide the state of node, which is shown in (1) is good, fair, or unsuited. Feedback values consist of minimum waiting time, link quality etc. An attacker now could struggle to quickly select a node give feedback values as response. Suitable selection for such events is framed, if the CTS are found having border line situations. The boundary conditions occur when value lesser than a particular threshold value is ignored or link quality exceeding particular threshold is opted.

$$ID = \begin{cases} \text{Good}, & \text{if } \begin{cases} \omega \le \omega^{Th} \\ \beta op \le \beta op^{Th} \\ T_r \ge T_r^{Th} \\ d_{RTS} \ge d_{RTS}^{Th} \\ E_{re} \ge E_{re}^{Th} \end{cases} \\ \text{Fair}, & \text{if } \begin{cases} \omega^{min} \le \omega \le \omega^{Th} \\ \beta op^{Th} < \beta op \le \beta op^{max} \\ T_r^{min} \le T_r < T_r^{Th} \\ d_{RTS}^{min} \le d_{RTS} < d_{RTS}^{Th} \\ E_{re}^{min} \le E_{re} < E_{re}^{Th} \end{cases} \\ \text{Unsuited}, & \text{if Otherwise} \end{cases} \quad (1)$$

$$T_q^p = f(\pounds, \emptyset) \quad (2)$$
$$\pounds = h(\beta 1, \beta 2, \beta 3, \beta 4, \beta 4, \beta 5, \beta 6) \quad (3)$$
$$\emptyset = i(\sigma 1, \sigma 2) \quad (4)$$
$$O = k(Bc, Erem) \quad (5)$$

Where;
β1 = is packets dropped by q which are sent by p
β2 = is total packets dropped by q
β3 = due to congestion packets dropped by q
β4 = due to unidentified reasons packets dropped by q
β5 = p's valuation of q's priority to q's self-packet vs. all other nodes packet
β6 = packets forwarding delay by q
σ1 = packets misrouted by q
σ2= packets falsely inserted by q.
Bc =remaining Buffer capacity
Erem= remaining energy
The chosen forwarding node (cluster head), is then permitted to continue with next phase. When cluster member transfer data to selected node. On completion of the data transmission process, the cluster head is evaluated using the factors like $\mathcal{T}$, $S_{Sr,}$.

Based on this evaluation Cluster Head will be rated as trusted, distrusted, uncertain which is shown in (5).

Reputation of node is represented by R. Using that R value here we update value of T. T the trust value is computed using (2). Trust value existence in (1) viewpoints initialized T values. During successive repetition of routing process, value of T is updated which is given in (5). To select best threshold value for trust we can use maximum false positive and minimum false negative rate. Literature given in [14-16] has taken nearly half trust value if extreme value is one. Based on criteria mentioned they have taken value in between 0.4 to 0.8. Furthermore, Nodes success ratio in packet delivery is represented by S_{Sr} and data transmission time is measured by τ . This analysis finds trustworthiness of node in some future unexpected communication. Some examples of attacks are data holding by malicious node, all or some data dropping before sending, which degrade the performance of network. Using $S_{Sr,}\mathcal{T}$ trust value is adjusted.

The proposed trust based secure routing pulls multiple parameters from several layers. These parameters are capable of identifying and reducing the outcome of different attacks like blackhole, Sybil, grayhole and sinkhole. But not all because rapid development of new security threats to network.

$$R = \begin{cases} Trusted(T_r \geq T_r^{Th}) & if \begin{cases} Ssr < Ssr^{Th} \\ \mathcal{T} \leq \mathcal{T}^{Th} \end{cases} \\ Uncertain(T_r^{min} \leq T_r < T_r^{Th}), & if \begin{cases} Ssr^{min} \leq Ssr < Ssr^{Th} \\ \mathcal{T}^{Th} \leq \mathcal{T} < \mathcal{T}^{max} \end{cases} \\ Distrusted & Otherwise \end{cases} \quad (6)$$

Fuzzy logic system is used to create feedback mechanism during cluster head selection and packet exchange phase for reliable packet delivery [2].

1. To be CH sends three values (remaining energy, nodes proximity with neighboring nodes , Link quality indicator).
2. Each node within the range of to be CH ask for different parameters like ω, βop, Tr , d_{RTS} , E_{re} .
3. To be CH sends CTS piggybacking the asked parameters.
4. CM calculates ID using (1).
5. Based on value of ID, CM will select CH
6. Data transmission phase
7. CM analyze CH under parameter by S_{Sr} and τ and then rate the CH given in (5).
8. CM will update trust value of CH

Algorithm for CH trustworthiness is given below.

B. Cluster Member Trustworthiness

When cluster member(CM) want to send data to cluster head, cluster head will check trustworthiness of cluster member because cluster member can also be compromised. Here we used distinctive attributes of MAC layer. These are number of times medium accessed by cluster member and time period of medium access control of each cluster member. If attacker node wants to deplete the energy of cluster head, then that attacker node will access the medium more often. So, now we work on MAC layer (medium access/sec all node). [1]

$$S = \begin{cases} Trusted & if \begin{cases} MAC_N < Th_{macn} \\ MAC_D < Th_{macd} \end{cases} \\ Uncertain & if \begin{cases} Th_{macn} \leq MAC_N < MAC_{Nmax} \\ Th_{macd} \leq MAC_D < MAC_{Dmax} \end{cases} \\ Detrusted, & if\ Otherwise \end{cases} \quad (7)$$

Cluster member is analyzed by cluster head based on medium access duration when CM frequently sending data. Parameter used for analysis is MAC_D medium access duration and then decided it is trusted, uncertain and distrusted as in (7).

M trustworthiness is given below.

1. CM send RTS to CH.
2. CH check number of medium access and MAC duration of CM.
3. Based on (7) CH will decide that CM is trusted , distrusted or uncertain.

IV. RESULT AND DISCUSSION

To evaluate the efficiency of proposed protocol, here we have done comparison for parameter like PDR (Packet delivery ratio), End to End delay and Energy consumption with and without using proposed method and also done comparison with TruFix. Parameters used for simulation are Antenna using two Ray Ground / Omni Directional , Layer- MAC – Adaptive MAC using Cross Layer , Communication Range is 1000 x 1000, Model- Energy Model, node count - 100 heterogeneous , Algorithm - Energy Efficient Fuzzy Based Cross Layer Protocol (EEFCLP), constant bit rate- 100 packets, payload size- 32 bytes. Figure 1,2,3 shows Packet delivery ratio with and without using trust based method , Energy consumption with and without using trust based method and end to end delay with and without using trust based method respectively where we have done comparison between with and without using trust based method . Figure 4, 5 and 6 compares proposed method with latest trust based protocol TruFix. Proposed method gives higher PDR when traffic is low and when increases interference and congestions traffic increases which reduce PDR but due to consideration of parameter remaining energy and the buffer occupancy period, we can gain considerable packet loss which occurred due to congestion and not due to attack. Another factor which affects PDR and energy consumption is source node trustworthiness

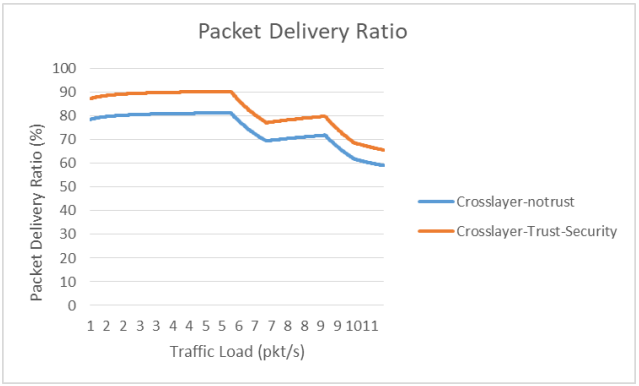

Fig.1. Packet Delivery Ratio with and without using Trust Security

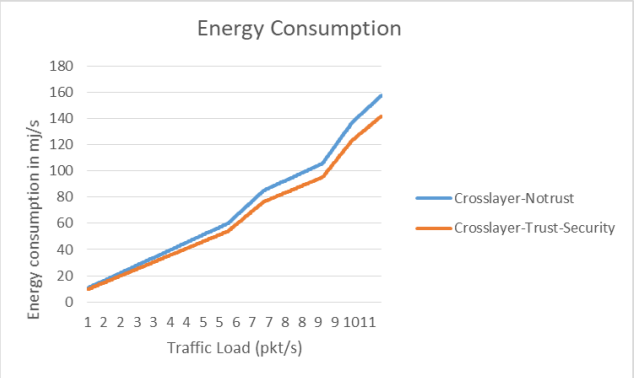

Fig. 2. Energy Consumption with and without using Trust Security

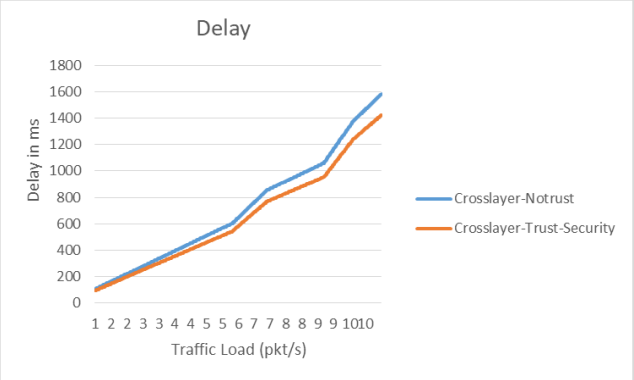

Fig. 3. Delay with and without using Trust Security

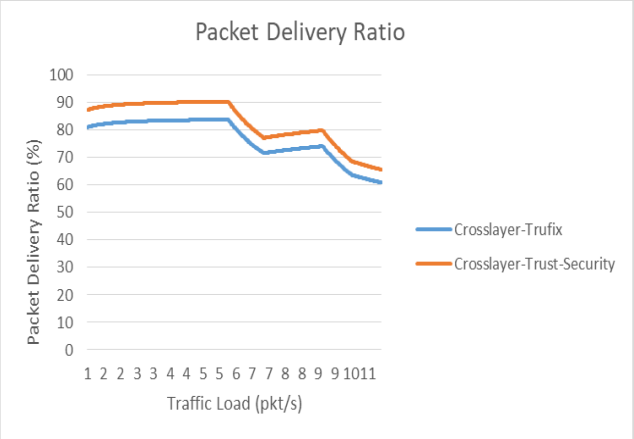

Fig 4. Packet Delivery Ratio for proposed Trust Security and Trufix

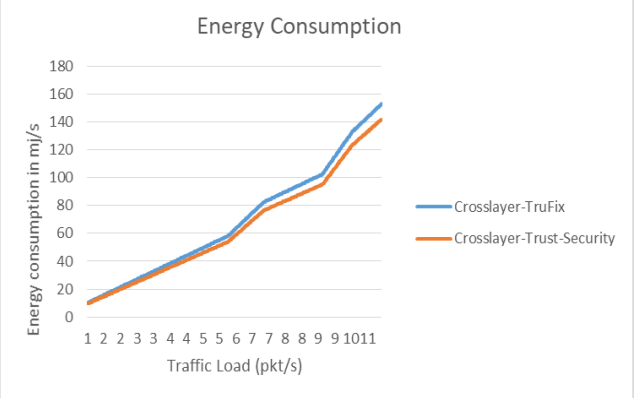

Fig. 5. Energy Consumption for proposed Trust Security and Trufix

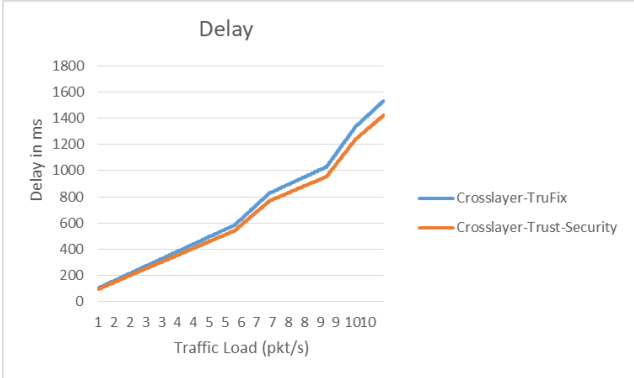

Fig. 6. End to End Delay for proposed Trust Security and Trufix

V. CONCLUSION

The proposed work trust based secure routing using cross layer method, is an enhanced work of Energy Efficient Fuzzy based Cross layer Protocol (EFCLP), which lacks security. Cross layer features are used which detects multiple layer attacks and this method conserve energy also. This proposed method detect misbehaving node at both source and destination end. Simulation experimentation done to show the effectiveness of this method. Simulation results shows that proposed method performs better in terms of energy, PDR, network lifetime and end to end delay after attack. Proposed method is compared with other secure routing protocol TruFix, which uses flat network and consider only forwarding misbehaving node .Simulation shows that proposed Trust based method performs better in terms of security and energy.

REFERENCES

1. L. Gandhimathi and G. Murugaboopathi, "Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-5. doi: 10.1109/ICICES.2016.7518935
2. I. A. Umar, Z. M. Hanapi, A. Sali and Z. A. Zulkarnain, "TruFiX: A Configurable Trust-Based Cross-Layer Protocol for Wireless Sensor Networks," in IEEE Access, vol. 5, pp. 2550-2562, 2017. doi: 10.1109/ACCESS.2017.2672827
3. H. Füßler, J. Widmer, M. Käsemann, M. Mauve, and H. Hartenstein, ‘‘Contention-based forwarding for mobile ad hoc networks,’’ Ad Hoc Netw., vol. 1, no. 4, pp. 351–369, 2003.
4. B. Karp and H. T. Kung, ‘‘GPSR: Greedy perimeter stateless routing for wireless networks,’’ in Proc. ACM 6th Annu. Int. Conf. Mobile Comput. Netw., 2000, pp. 243–254.
5. M. C. Vuran and I. F. Akyildiz, ‘‘XLP: A cross-layer protocol for efficient communication in wireless sensor networks,’’ IEEE Trans. Mobile Comput., vol. 9, no. 11, pp. 1578–1591, Nov. 2010.
6. Ali Ghaffari, An Energy Efficient Routing Protocol for Wireless Sensor Networks using A-star Algorithm, Journal of Applied Research and Technology, Volume 12, Issue 4, 2014, Pages 815-822, ISSN 1665-6423, https://doi.org/10.1016/S1665-6423(14)70097-5.
7. S. B. Lande and S. Z. Kawale, "Energy Efficient Routing Protocol for Wireless Sensor Networks," 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), Tehri, 2016, pp. 77-81. doi: 10.1109/CICN.2016.22
8. Dhage MR, Vemuru S. A Effective Cross Layer Multi -Hop Routing Protocol for Heterogeneous Wireless Sensor Network. Indonesian Journal of Electrical Engineering and Computer Science . 2018 May 1; 10(2): 664 -671

9. Farruh Ishmanov and Yousaf Bin Zikria, "Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues," Journal of Sensors, vol. 2017, Article ID 4724852, 16 pages, 2017. https://doi.org/10.1155/2017/4724852.
10. F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, ''Trust management system in wireless sensor networks: Design considerations and research challenges,'' Trans. Emerg. Telecommun. Technol., vol. 26, no. 2, pp. 107–130, 2015.
11. J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: a trust- aware secure routing framework in wireless sensor networks," International Journal ofDistributed Sensor Networks,vol.2014, Article ID 209436, 14 pages, 2014.
12. Eid Rehman, Muhammad Sher, Syed Hussnain Abbas Naqvi, Khan Badar Khan, and Kamran Ullah, "Energy Efficient Secure Trust Based Clustering Algorithm for Mobile Wireless Sensor Network," Journal of Computer Networks and Communications, vol. 2017, Article ID 1630673, 8 pages, 2017. https://doi.org/10.1155/2017/1630673.
13. R. Ferdous, V. Muthukkumarasamy, and A. Sattar, ''Trust formalization in mobile ad-hoc networks,'' in Proc. IEEE 24th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA), Apr. 2010, pp. 351–356.
14. A.Jøsang, R. Ismail,and C. Boyd,"A survey of trust and rep- utation systems for online service provision," Decision Support Systems, vol. 43, no. 2, pp. 618–644, 2007.
15. C. J. Fung, J.Zhang, I.Aib, R.Boutaba, and R. Cohen, "Design of a simulation framework to evaluate trust models for collaborative intrusion detection," in Proceedings of the International Conference on Network and Service Security (N2S '09), pp. 13–19, IFIP, Paris, France, June 2009.
16. F. Ishmanov, S. W. Kim, and S. Y. Nam, "A robust trust establishment scheme for wireless sensor networks," Sensors, vol. 15, no. 3, pp.7040–7061, 2015.

AUTHORS PROFILE

Mrs. M. R. Dhage is a part time research scholar in Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, 522502, Andhra Pradesh, India .Currently she is working in Sinhgad College of Engineering, Pune, Maharashtra, India. She has published more than 20 research papers, her current research interests include energy efficiency and secure routing algorithms and network survivability in wireless sensor networks

Dr. Srikanth Vemuru is a Professor & Dean- Skill Development in Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, 522502, Andhra Pradesh, India. He has published more than 90 research articles. His research interests are in the areas of energy conservation in Sensor Network, MAC protocol, Cognitive radio, and underwater sensor networks.