Science and Technology Journal Vol. 7 Issue: 2 July 2019 ISSN: 2321-3388

A Novel Framework to Secure CBWSNS Against the Selfishness Problem

Poonam Mittal
CE Department, J.C. Bose University of Science & Technology, YMCA, Faridabad, India
E-mail: poonamgarg1984@gmail.com

Abstract—Dynamic and cooperative nature of sensor nodes in Wireless Sensor Networks raises question on security. Various researchers work in this direction to spot malicious, selfish and compromised nodes. Various mechanisms followed are uniqueness of clustering, reputation system and an operation at specific nodes. LEACH is a hierarchical protocol in which most nodes transmit to cluster heads, and the cluster heads aggregate and compress the data and forward it to the base station (sink). Each node uses a stochastic algorithm at each round to determine whether it will become a cluster head in this round. Clustering process carried out in two stages takes the role of the reputation scheme and reveals specific operation at CH, IN and MNs beside their usual activities in cluster based wireless sensor networks. This paper mentioned the final structure of the security framework, corresponding attacks and defense mechanism of the model. It also discusses various security level processes of wireless sensor networks. Results implies that in a cluster-based protocol such as LEACH in which optimally 5% of the nodes are cluster heads it is likely that a significant portion of the network can be paralyzed or the entire network disabled, in the worst-case scenario, if these cluster heads are compromised. Our main contribution in this paper is our novel approach in maintaining trusted clusters through a trust-based decision-making cluster head election algorithm.

Keywords: *WSNs, Selfish Attack, Security Schemes, Trust, Cluster, LEACH*

INTRODUCTION

Wireless Sensor Networks (WSN) are vulnerable to internal and external attacks as a result of collaborative and dynamic nature of the network having sensor nodes with less memory and low power devices (Yick *et al*. 2008; Akyildiz 2002). Many crypto-logical algorithms were accessible for generic enhanced securities but most of them are not appropriate for wireless sensor networks. As cryptography mechanisms are not enough to prevent any internal attacks, as well as not able to differentiate between malicious node or selfish, behavior of nodes (Mittal *et al*. 2015; Schaffer *et al*. 2012; Dong *et al*. 2009). But this mechanism is not capable to secure the complete network (no improvement of distributed knowledge gathering and cooperative data processing in the network). The main objective of the security framework for cluster based wireless sensor networks is to enhance the general performance by monitoring network activities like like information gathering and information processing and minimizing the risk (Thein *et al*. 2008). A security framework for Cluster- Based Wireless Sensor Networks (CBWSNs) was introduced (Ishaq *et al.* 2015) to deal the security issue as shown in figure 1.

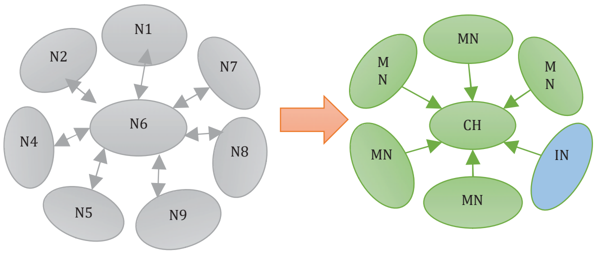

Fig. 1: WSN-before and after Cluster Formation

In this secured framework two special nodes per cluster are appointed: investigation node and cluster head node. In every cluster three types of nodes are formed CH, IN, and MNs (member nodes) and these nodes are one hop apart from CH as shown in Figure 1. In order to control the selfishness attack (Nagpal 2016; Kanchan *et al*. 2014; Yoo *et al*. 2006), a security mechanism is provided by using a reputation system at every node. The IN node

https://doi.org/10.22232/stj.2019.07.02.01

exploits the packet overhearing scheme, that is one among the characteristics of wireless communication and utilized by several previous researches to supply security against the selfishness attack ensures entity as secure and reliable, so security model is used to differentiate trust-worthy and unreliable nodes in a network. It encourages trustworthy nodes (Nagpal 2016) to speak and discourages unreliable nodes to participate within the network.

Also, it increases the network life time, throughput and resilience of the wireless sensor network. There are three types of selfish nodes as follows:

1. ***Selfish CH:*** It drops information packets rather than forwarding to sink nodes.
2. ***Selfish IN:*** It stops overhearing CH or sends deliberate accusing messages on CH.
3. ***Selfish MNs:*** It does not properly participate within the CH and IN election method. It means it does not present itself for the IN nomination and additionally does not reply to CH selection method deliberately.

These nodes can behave absolutely or partly selfish, it means they do not perform their roles regularly or intermittently. For example, under partly selfish behavior, the information forwarding of CH, overhearing of IN, and participation of MNs in election method can be stopped intermittently. On the opposite hand, if these activities are stopped for a protracted while, then nodes can be thought of as absolutely selfish or dangerous.

Various security frameworks against selfish attack with existing schemes for the safety of cluster head election, specializing in the schemes. The common goal of these schemes is to produce security for cluster head node election against active attacks by using various technologies. However, they met with many limitations. Recent security proposals were discussed in the following section.

VARIOUS SECURITY SCHEMES IN WIRELESS SENSOR NETWORKS

Brief of various security mechanisms to secure CBWSNs is discussed in Table 1.

Table 1: Literature Review

Title	Methodology	Objective	Performance Matrix
Impact of a simple load balancing approach and an incentive-based scheme on MANET performance (Yoo *et al.* 2010).	Incentive Scheme	Resolve the selfishness attack	They participated in a cooperative environment
A lightweight and dependable trust system for clustered wireless sensor networks (Li *et al*. 2013)	Trust System	Providing collaboration among trustworthy nodes	An identifying misbehavior nodes
A survey of trust and reputation management systems in wireless communications (Yu *et al*. 2010)	Reputation and Trust System	To avoid beings a victim of inside attacks	Encourage the nodes to be honest by giving some credits
Trust among strangers in internet transactions: empirical analysis of eBay's reputation system (Resnick and Zeckhauser 2002)	Reputation and Trust System	To avoid beings a victim of inside attacks	Encourage the nodes to be honest by giving some credits
Using overhearing technique to detect malicious packet-modifying attacks in wireless sensor networks (Ssu *et al.* 2007)	Centralize Scheme	Mitigate the selfishness problem in CBWSNs	Maximizing the life time and minimizing selfishness attack.
SecLEACH-on the security of clustered sensor networks, Signal Processing (Oliveira *et al*. 2007)	Distributed Scheme	Avoid the single point of failure	Excessive use of resources
Performance evaluation of wireless sensor network under black hole attack (Gulhane and Mahajan 2014)	Overhearing Scheme	Captured black hole region and blocked	Easily monitored and controlled by IN
Queuing the trust: Secure backpressure algorithm against insider threats in wireless networks (Lu *et al*. 2015)	Data overhearing scheme	Resolve selective forwarding attack	Detected and controlled transmission of CH

The common goal of these schemes is to produce security for cluster head node election against active attacks by using various technologies. However, these techniques met with many limitations. First, they can handle only active or external attacks; second, they are centralized schemes, employing a base station to form a decision about the head nodes. Hence, they are not appropriate for WSNs. Third, the 3 election protocols in (Chowdhury *et al*. 2014) use light-weight crypto-graphical algorithms, but they are vulnerable to various attacks. Lastly, the protocols in [27] using digital signatures involve considerable computation overhead and area unit susceptible to DoS attacks, being not appropriate for resource restricted little WNS nodes. So there is a strong need to deal the severe issues of WSN security discussed above.

PROPOSEDWORK

Aim of this protocol is to choose trusted CH i.e. nodes with less trust value or less energy should not be selected as CH. Proposed work can be divide into two main modules that is trust based routing module and trust management module. Figure 2 represents overall architecture of proposed algorithm.

- ***Trust Management Module*****:** This module calculates trust based upon remaining energy, PDR and distance.
- ***Trust-based Routing Module*****:** It is almost same as basic LEACH protocols with some changes in it. Trust-based routing module uses trust management module to perform secure routing.

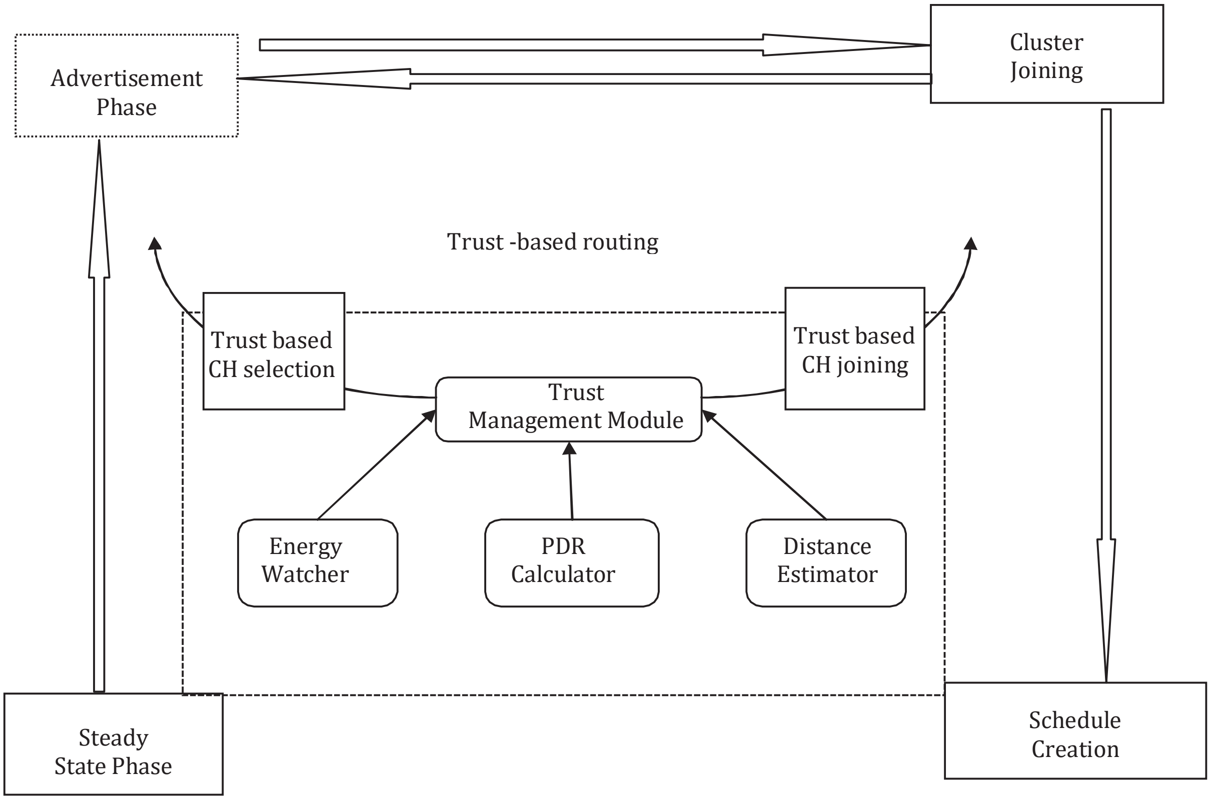

Fig. 2: System Architecture

An improvement in clustering protocol has been proposed, while maintaining the routing of original LEACH protocol. The scheme used to calculate trust is described below:

Inputs:

- Network area.
- Number of nodes.

Assumptions

For executing reputation mechanism for sensor networks environment, following assumptions have been made:

- There are some selfish nodes present in the network.
- BS has unlimited source of energy and it is free from any kind of attack.
- If a node is performing some selfishly then it will be penalized and its reputation value will decrease.
- If a node is showing good behaviour, it will be rewarded and its reputation value will be increased.
- Selfish nodes present in network are consuming more energy and dropping more packets than normal nodes.

Nodes will be randomly distributed in given area. Every node runs with an energy watcher, PDR calculator, distance estimator and trust supervisor. Energy Watcher will calculate remaining energy of neighbor nodes and CHs, PDR calculator will calculate PDR of every node based upon number of packets dropped by node, Distance Manager will calculate and maintain distance between node and neighbors node along with CH distance with node Trust Supervisor will maintain trust level of neighboring nodes and CHs elected by considering three factors that are remaining energy, PDR and distance between nodes. For calculating trust value three factors will be considered that are remaining energy, PDR and distance i.e. nodes with high remaining energy, high PDR, and less distance between nodes will have more trust value and thus have high chances of becoming CH as compared to those nodes with low trust value, low PDR and high distance between nodes. These four components will work as follows:

Energy Watcher: It will keep track of remaining energy of nodes. Energy model for the network is discussed as: To transmit a k-bit message with a distance of d, energy consumption can be calculated by:

$$E_t = E_e\,(k, d) + E_a\,(k,d) \qquad (1)$$

Where E_t is the transmitting energy, E_e is energy required to run transmitter and receiver circuitry, E_a is transmitter amplifier energy and energy required to receive any packet can be calculated by:

$$E_r = K * E_e \qquad (2)$$

Hence energy will be consumed while transmitting or receiving packets in the network. As sensor networks are deployed in area where it is not possible to charge these nodes timely, so protocol designed should be energy efficient to save energy of these nodes and increasing network lifetime.

- ***PDR Calculator:*** This component will keep track of PDR. From the past records PDR calculator will maintain total number of packets sent to BS and how many of them are actually received by BS. Packets may be intentionally dropped by selfish node.
- Another reason for packets drop may be poor network connectivity. Node with high PDR will have high trust value and node with low PDR will have less trust value. Formula for PDR can be given as:

  Packet_Delivery_Ratio = Packets_Rcvd/Packets_TO_BS (3)

  Where, Packets_Rcvd are total number of packets received by BS

  Packets_TO_BS are total number of packets sent to BS.
- ***Distance Estimator:*** This component will keep track of distance between nodes. If distance between evaluated node and subject node is less, a high trust value will be assigned to evaluated node otherwise if distance between subject node and evaluated node is high, then low trust value will be assigned to node. Hence trust value is inversely proportional to distance between nodes. Also this component will keep track of distance between nodes and CH.
- ***Trust Supervisor:*** This component will maintain trust values of nodes that will be used by routing module for trusted CH election and secure routing. The working of trust supervisor is being discussed in trust management module.

Trust Management Module

For calculating trust, trust supervisor will calculate both direct and indirect trust and final trust will be calculated by aggregating both trust values. Direct trust is that trust which is calculated by nodes itself. Direct trust will be calculated based on past and present interactions of nodes. Sometimes it is not possible for a node to calculate direct trust of other nodes in order to save energy; in that case nodes will take recommendations from other nodes which will result in indirect trust. Indirect trust is also called second hand trust. In this model trust is calculated by considering energy, distance and PDR as trust metric. Nodes with high remaining energy, high PDR, less distance between nodes will have more trust value as compared to those nodes with less remaining energy, less PDR, more distance between nodes. As shown in figure 3 a subject node is one which wants to calculate trust of other node, evaluated node is one whose trust value is to be calculated, recommendation nodes are those whose opinions are considered for calculating in direct trust.

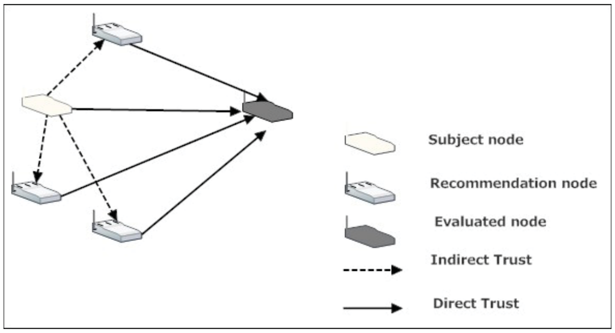

Fig. 3: Trust Relationship

An initial trust of 0.5 is assigned to every node. For calculating direct trust, trust supervisor will interact with energy watcher, PDR calculator and distance estimator. For calculating direct trust, first trust supervisor will check remaining energy, and then a series of if-then rules will be applied to remaining energy, by comparing remaining energy with threshold value trust values will be assigned to nodes. Threshold values are selected by analyzing remaining energy after a particular round. Nodes will be awarded or penalized based upon the results after comparing remaining energy with threshold value. A node will be rewarded if its remaining energy is high after a particular round and if at the same round node is having less energy as compared to threshold then it will be penalized.

Once remaining energy has been checked, next trust supervisor will check PDR of nodes. PDR of nodes is compared with thresholds and then accordingly reward or penalty will be given. A node with high PDR will be rewarded and the nodes which drop more number of packets will have less PDR and hence penalized.

Further trust is dependent on another factor that is distance between nodes. If distance between nodes is high then corresponding trust of the node will be more and vice-versa. Hence direct trust can be calculated based upon aggregation of three factors.

Next, indirect trust will be calculated based on recommendations considered from other nodes. Indirect trust is the sum of trust values calculated by other nodes and given by equation 4.

```
Trust_Calculation ( )
Input: Remaining energy, Packet_delievery_ratio, Distance between nodes
    Every node is assigned with initial direct trust of 0.5
    if ($R.E > Th_1$)
    DT= DT+5%of DT//node will be rewarded
    elseif ($Th_2 < R.E < Th1$)
    DT=DT //trust will remain same
    elseif ($R.E < Th_2$)
    if ($PDR > Th_3$)
    DT=DT+5%of DT//node will be rewarded
    elseif ($Th_4 < PDR < Th_3$)
    DT=DT //trust will remain same
    elseif ($PDR < Th_4$)
    DT=DT-5%ofDT //node will be penalized
    End
    if ($D_{S.N \to E.N} > Th_5$)
    DT=DT+5%of DT//node will be rewarded
    elseif ($Th_6 < D_{S.N \to E.N} < Th_5$)
    DT=DT//trust will remain same
    elseif ($D_{S.N \to E.N} < Th_{6.}$)
    DT=DT-5%ofDT//node will be penalized
    End
    Indirect trust will be calculated from
    recommendation nodes.
    TT= w *DT + (1-w)*IT
    DT=DT-5%of DT//node will be penalized
    End
Notation: DT = Direct Trust
IT = Indirect Trust
TT = Total Trust
Th = Threshold Value
$D_{S.N \to E.N}$= Distance between subject node and evaluated node
```

Fig. 4: Pseudo Code for Trust_Calculation ( ) in CBWSNs

$$IT^{C}_{A\to B} = \sum\nolimits_{C} DT_{A\to C} \times DT_{C\to B} \tag{4}$$

Where, $IT^{C}_{A\to B}$ is indirect trust of B calculated by A considering recommendation from C and C ≠A; and $DT_{A\rightarrow C}$ are the direct trust value calculated by A for C and C forB.

For calculating final total trust both of direct and indirect trust will be aggregated as given below by 3.5:

$$TT_{A\rightarrow B} = wDT_{A\rightarrow B} + (1\text{–}W)\, IT^{C}_{A\rightarrow B} \qquad (5)$$

$TT_{A\rightarrow B}$ is the total trust of node A on node B, w is the weight associated with direct and indirect trusts. A higher value of w signifies that sensor nodes relies more on its own judgment whereas a lower value of w signifies that sensor nodes has more trust on recommendations provided by other nodes. Final trust values of nodes will be stored by Trust Supervisor.

Trust-based Routing Module

Routing module consists of two main phases: Set-up phase and Steady-state phase. In Set-up phase clusters are arranged and selected followed by steady-state phase where nodes will transmit data to BS.

Set-up Phase

a. ***Advertisement Phase****:* This phase is same as in original LEACH protocol but for increasing lifetime of network energy factor is considered while selecting CH, so that the nodes with less energy should not get selected as CH. The number of nodes elected as CH with low energy will be less thus increasing network lifetime. To start procedure of CH election, node will select a random number between 0-1. If the number chosen is less than threshold node, node will be selected as CH otherwise not. The threshold value can be given by equation 6.

$$T(n) = \frac{\substack{p \\ n\mathit{E}G}}{\text{I - pxr}\,\text{mod}(1/p)} \qquad (6)$$

Where p is the desired percentage of CHs, G is set of nodes that have not been elected as cluster-heads in the last 1/p rounds and r is the current round, is remaining energy of node and is initial energy of node. After this phase, nodes has list of all eligible CH members. After CH has been selected, now elected CH will find all its CH neighbors and all information regarding CH neighbor will be collected from energy watcher, trust supervisor and distance manager. CH will maintain information of neighbor CH in form of a table. Each node will maintain an entry corresponding to every attribute mentioned in table 2.

Table 2: Neighbor CH Information

Attribute	Description
ID	ID of neighboring CH
	Remaining energy of CH
	Final trust of neighboring CH
	Minimum distance of neighboring CH from BS
EC	How many times Neighboring CH is elected as CH
	Whether nearest neighbor or not

Now, CH will examine whether neighbor is nearest neighbor or not and this will be decided by comparing distance of nodes with D. Equation 7 gives the value of D. Distance between CHs will be calculated with signal strength. If distance calculated is less than D then

$N_{nearest}$ = 1else it is 0.

$$D = \acute{\alpha} \times \sqrt{\ } 1/\ \pi\, k \times L \qquad (7)$$

Where L is the side length of the square area where sensor nodes are deployed, K is the number of cluster-heads; is an adjusting factor. This will uniformly cover whole area CHs. If number of nearest neighbor CH is greater than 0 then CH will calculate trust weight associated with every nearest neighbor CH and trust weight, is calculated by equation 8.

$$W_T = \alpha \times E_{REM\,/}\, E_{INT} + \beta \times T_{node}\ / \\ \sum T_{node} + \gamma \times d(CH, BS)/AD_{C\rightarrow BS} + EC \qquad (8)$$

Where, α, γ, β are the weight factors selected accordingly. As for this thesis energy is already considered as attribute for trust calculation, so for simulation a lower value of α is considered. If some other attribute is selected then a higher value for α should be considered otherwise β can have higher value as trust value already considered energy factor and EC is number of times node is selected as CH. T_{node} is the trust value of neighboring CH obtained from trust management module. ∑ T_{node} is aggregation of trust of all nearest neighbor CH. CH with heaviest trust weight value is selected as new CH and will broadcast this information to other nodes and CH selected earlier will vanish. In addition, minimum distance of node from BS is also considered. CH distance to BS is compared with others nodes CH distance to BS and if difference between CH and BS is greater than predefined value, node will not be selected as CH. d(CH, BS) is distance calculated between CH and BS and $AD_{c\rightarrow BS}$ is the acceptable distance between CH and BS. Hence CH selected with this procedure will be trusted, with better energy and will help in saving energy as transmitting energy cost will be less.

a. ***Cluster Joining***: In original protocol non-CH nodes join cluster based on signal strength received from CH but here nodes will select their CH based on trust values of cluster nodes.

b. ***Schedule Creation****:* CH receives all messages from nodes that would like to join cluster. Based upon strength of nodes in the cluster, CH begins to create a TDMA schedule and assign slots to non-cluster nodes to send data as well as to calculate trust.

Steady State Phase

In steady state phase nodes will transmit sensed data to CH along with calculating trust. This phase can be divided into two slots data slots and trust slots [11] as shown in figure. After this phase every other round begins with set-up phase.

- ***Data Slots****:* Nodes will keep their transmitter on during their time slot only and will sense the data in the same time slot and send sensed data to CH selected meanwhile other nodes transmitters are off in order to save energy. It is assumed that CHs are having more energy than normal nodes so they keep their receivers always on to receive data from non-CH nodes.
- ***Trust Slots****:* During this slot trust supervisor will calculate trust associated with their neighbors based upon considered factors as well as CH. Nodes update trust value regularly. In addition, CH will calculate trust of neighbour CHs in this slot and updates their table.

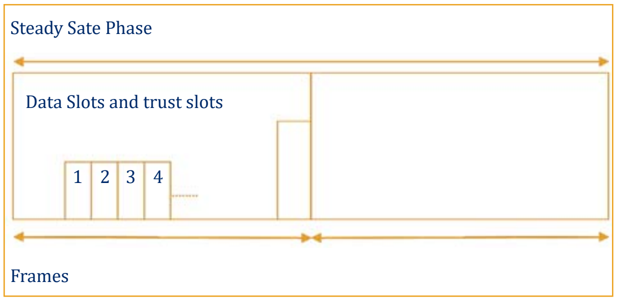

Fig. 5: TDMA Schedule

For communication within a cluster i.e. an intra-cluster communication, amplification energy must be less than a inter-cluster communication that is a communication between CH and BS [22]. The reason behind this is within a cluster distance between nodes is less, so less of energy is needed to transmit a message as compared to inter-cluster communication. Therefore more energy could be saved.

```
Nodes will be randomly placed in an area.
forr=1:1:n
fori=1:1:n
temprand =rand // a random value between 0-1 well be chosen
if (temp_rand <=((p/(1-p*mod(r, round(1/p))*$E_{rem}/E_{int}$))))
Then CH will be selected
Total_trust=Trust_Calculation()// nodes will calculate trust of other nodes
CH will find its close neighbour
D=phi*sqrt(1/pi/K)*L;
if ((distance between CH and close neighbour CH)<D)
then $N_{close}$=True
else $N_{close}$=False
N=count number of close CH neighbour
if(N>0)
Then Compute weight of each close neighbour
Node with heaviest weight factor will be selected as trusted CH
Nodes will join the CH with maximum weight value
```

Notations:

r= Number of rounds

n= Total number of nodes

Fig. 6: Pseudo Code for Routing Module in CBWSNs

IMPLEMENTATION

The proposed algorithm CBWSNs has been designed in MATLAB [15]. It is considered that 100 nodes are randomly distributed over area of 100*100 m^2. Firstly basic LEACH is implemented. Sensor nodes send data to CH, CH after aggregating the data from cluster members further route it to BS. To study better results of trust management scheme some selfish nodes are introduced in network. It is assumed that selfish nodes are consuming high energy and dropping packets. It may be possible that selected CH is selfish which will drop packets that were supposed to send to BS i.e. selfish nodes defined in the network are launching selective forwarding attack. After implementing trust management scheme, chances of selecting malicious CH is almost negligible which will enhance network performance. Hence, proposed scheme is energy efficient, so network lifetime is improved with this scheme. In addition CH with heaviest trust weight is selected, so probability of packets drops ratio is decreased.

Evaluation is done based upon following metrics:

- Network life time.
- PDR

Simulator parameters are mentioned in table 3.

Table 3: Simulation Parameters

Network Parameters	Values
Network Size	100X100m^2
Number of nodes	100
Packet Size	4000 bits
Routing Protocol	LEACH
Initial battery power of node	0.5 J/node
Energy to run transmitter and receiver	50 nJ/bit
Data aggregation energy	5 nJ/bit
Amplification Energy (Cluster to BS)	Efs =10pJ/bit/m^2
Amplification Energy (Intra Cluster Communication)	Efs/10 = Efs$_1$

Simulation Results

Selection of CH

Figure 7 shows random distribution of sensor nodes in an area of 100*100 sq. units and LEACH protocol is simulated for routing purpose.

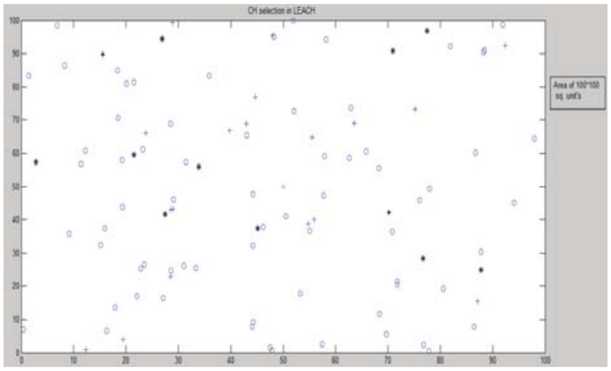

Fig. 7: CH Selection in LEACH

There are some malicious nodes present in the network. Malicious nodes are represented by a plus (+) sign, normal nodes are represented with a circle (o). In addition selection of CH in particular round is also presented in figure 7. Nodes that are selected as CH are represented with dark blue asterisk. It can be easily analyzed that if no security practices are adopted, selfish nodes present in network could be selected as CH. Hence as a result malicious CH selected would drop packets received from cluster members which in result reduce network performance. After implementing CBWSNs, it is verified that chances of selecting selfish nodes as CH are almost negligible. In CBWSNs, CH is selected based upon trust values of nodes. Therefore selected CH will not be malicious. The whole scenario is represented in figure 8. Trusted CH selected is represented by Green asterisk.

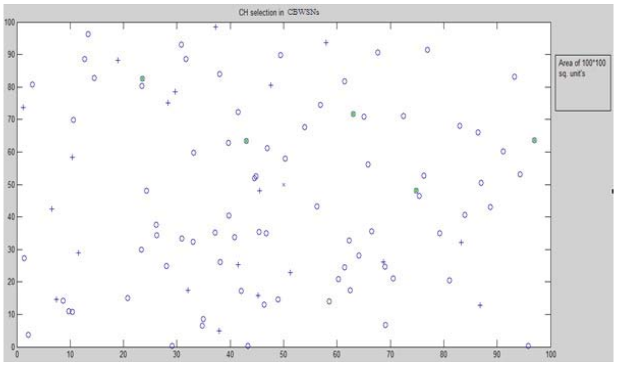

Fig. 8: CH Selection in CBWSNs

Trust Evolution

Figure 9 plots trust value of a selfish node. Trust value of a selfish node decreases as time increases. The value of $_w$ is selected chosen to be 0.5 in equation 6 which concludes that node is equally considering direct trust as well as recommended trust and value of α, β, γ are selected to be 0.2, 0.6, 0.2 in equation 9.

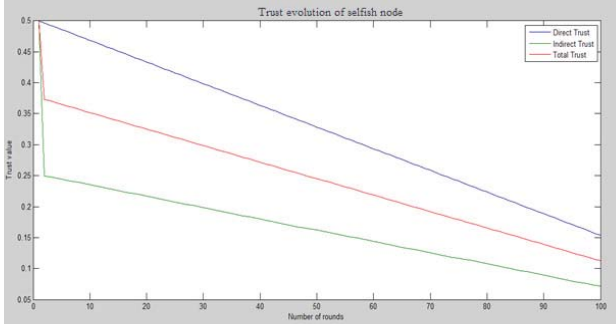

Fig. 9: Trust Evolution of a Selfish Node

At very first round node will have direct trust of 0.5, no indirect trust will be considered at first round, hence total trust will constitute to 0.5. Similarly at 10th round direct trust is 0.4800, indirect trust is 0.2438 and thus total trust is 0.3619 for this round. In the proposed model calculated trust is directly proportional to remaining energy and PDR, as malicious node consumes more energy, drops more packets therefore its trust value decreases as number of round increases.

Analysis of PDR

Figure 10 shows number of selfish node versus average PDR. It could be observed that average PDR is 96% in CBWSNs and 91% in LEACH when there is no malicious node present in the network. There would be some packet loss because of poor network connectivity. Therefore PDR would not be 100% even if no selfish node present in the network. With presence of 5 selfish nodes in network CBWSNs network has PDR value of 0.9400 and LEACH has 0.8390, hence after implementing CBWSNs PDR increases by 12%. Similarly when 15 selfish nodes are present PDR is increased by 14% and with presence of 25 selfish nodes PDR increases by 21.5%. Hence it could be concluded that after implementing CBWSNs average PDR ratio is increased by 15.8%. CBWSNs have high average PDR as compared to leach because selfish nodes are not selected as CH and hence there are less packet drop in the network. Moreover CBWSNs can help in avoiding selective forwarding attack.

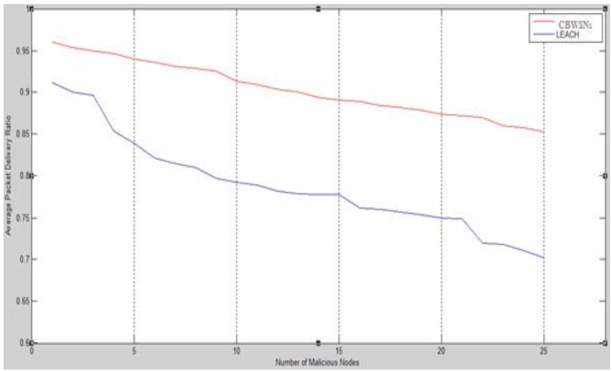

Fig. 10: PDR *vs.* Number of Selfish Node

Network Lifetime Comparison

While comparing network lifetime it has been observed that CBWSNs has better lifetime as compared to LEACH. As in LEACH there are many retransmissions as compared to CBWSNs, in addition in CBWSNs less of malicious nodes would be selected as CH so less consumption of energy as it is assumed that malicious nodes are consuming more energy. Moreover, consumption of less energy while intra-cluster communication as compared to inter-cluster communication and consideration of energy factor while selecting CH makes CBWSNs more energy efficient. It could be verified from figure that in LEACH first node dies near 700th rounds as compared to CBWSNs where first node dies at 1100th round. Figure 11 shows network life time comparison.

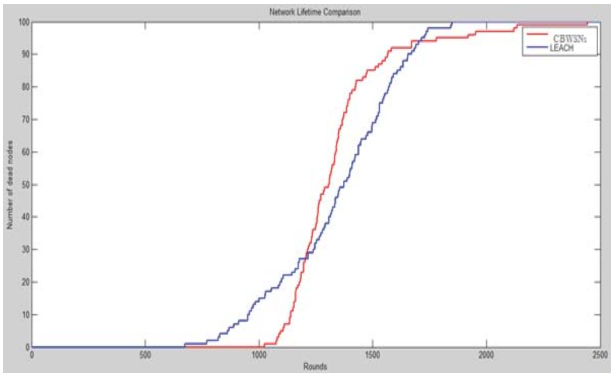

Fig. 11: Network Lifetime

CONCLUSION

An energy efficient trust based approach has been proposed which is combination of trust-based routing module and trust management module. In trust management module, trust supervisor calculates trust for nodes as well CH that can be used for trusted CH selection and secure routing. Total trust value is a combination of direct trust that is calculated by node itself and indirect trust which is trust from recommendation nodes. Trust-based routing module modifies original Clustering. Routing module comprises of further four phases that are advertisement phase, cluster joining, schedule creation and steady state phase. Nodes that are selfish in nature will have less PDR and consumes more energy. So these selfish nodes will not be selected as CH because their computed trust value will be less. In addition, routing module uses less energy for intra-cluster communication as compared to inter-cluster communication which would help in improving network life time.

Protocol performance is verified using MATLAB simulator. It is verified that selfish nodes will not be selected as CH and trust value of a malicious node decreases with time. Simulation results proved that proposed algorithm consumes less energy and improves PDR as there are less number of retransmission. Average PDR is improved by 15.8%. In addition with implementation of CBWSNs, network lifetime improves as first node dies at 1100th round in CBWSNs as compared to LEACH where first node dies at 700th round.

REFERENCES

Yick J, Mukherjee B, Ghosal D (2008) Wireless sensor network survey: Computer networks 52: 2292-2330.

Akyildiz I F, Su W, Sankarasubramaniam Y, Cayirci E (2002) A survey on sensor networks: IEEE Communications magazine 40: 102-114.

Younis O, Krunz M, Ramasubramanian S (2006) Node clustering in wireless sensor networks: Recent developments and deployment challenges: IEEE network 20: 20-25.

Kumarawadu P, Dechene D J, Luccini M, Sauer A Algorithms for node clustering in wireless sensor networks: A survey. In *2008 4th International Conference on Information and Automation for Sustainability* (pp. 295-300). IEEE.

Abbasi A A, Younis M (2007) A survey on clustering algorithms for wireless sensor networks: Computer communications 30: 2826-2841.

Mittal P, Batra S, Nagpal C K(2015) Implementation of a novel protocol for Coordination of nodes in MANET: International Journal of Computer Networks and Applications 2: 99-105.

Schaffer P, Farkas K, Horváth Á, Holczer T, Buttyán L(2012) Secure and reliable clustering in wireless sensor networks: A critical survey: Computer Networks 56: 2726-2741.

Dong Q, Liu D. Resilient cluster leader election for wireless sensor networks. In2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks; IEEE; 2009. pp. 1-9.

Thein T, Chi SD, Park JS. Increasing availability and survivability of cluster head in WSN. In 2008 The 3rd International Conference on Grid and Pervasive Computing-Workshops; IEEE; 2008. pp. 281-285.

Yan M, Xiao L, Du L, Huang L. On selfish behavior in wireless sensor networks: a game theoretic case study. In 2011 Third International Conference on Measuring Technology and Mechatronics Automation; IEEE; 2011. pp. 752-756.

Yoo Y, Agrawal D P (2006) Why does it pay to be selfish in a MANET?: IEEE Wireless Communications, 13(6): 87-97.

Yoo Y, Ahn S, Agrawal D P (2010) Impact of a simple load balancing approach and an incentive-based scheme on MANET performance: Journal of Parallel and Distributed Computing 70: 71-83.

Li X, Zhou F, Du J (2013) LDTS: A lightweight and dependable trust system for clustered wireless sensor networks: IEEE Transactions on Information Forensics and Security 8: 924-935.

Yu H, Shen Z, Miao C, Leung C, Niyato D. A survey of trust and reputation management systems in wireless communications. Proceedings of the IEEE; 2010. pp. 1755-1772.

Resnick P, Zeckhauser R (2002) Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system: The Economics of the Internet and E-commerce 11: 23-25.

Nagpal C K (2018) A game theory based solution for security challenges in CRNs: 3D Research 9:11-23.

Nagpal C K (2016) A Novel Technique to Prevent PUE Attack in Cognitive Radio Network: International Journal of Computer Network and Information Security 8: 44-50.

Kanchan S, Mittal P, Nagpal C K (2014) Effect of Enhancing MAC layer Security and Power Saving Mode on Mobile Ad Hoc Network: International Journal of Computer Science and Engineering Technology 5: 784-791.

Ssu K F, Chou C H, Cheng L W (2007) Using overhearing technique to detect malicious packet-modifying attacks in Wireless Sensor Networks: Computer Communications 30: 2342-2352.

Ishaq Z, Park S, Yoo Y. A security framework for Cluster-based Wireless Sensor Networks against the selfishness problem. In 2015 Seventh International Conference on Ubiquitous and Future Networks; IEEE; 2015. pp. 7-12.

Chowdhury A R, Chatterjee T, Bit SD. LOCHA: A Light-weight One-way Cryptographic Hash Algorithm for Wireless Sensor Network; ANT/SEIT; 2014. pp. 497-504.

Oliveira L B, Ferreira A,Vilaça M A, Wong H C, Bern M, Dahab R, Loureiro A A (2007). SecLEACH—On the Security of Clustered Sensor Networks: Signal Processing 87: 2882-2895.

Gulhane G, Mahajan N (2014) Performance evaluation of Wireless Sensor Network under black hole attack: International Journal of Computer and Technology 1: 92-96.

Lu Z, Sagduyu YE, Li JH. Queuing the trust: Secure backpressure algorithm against insider threats in wireless networks. In 2015 IEEE Conference on Computer Communications; IEEE; 2015; pp. 253-261.