# DYNAMIC WATCHDOGS USING AODV PROTOCOL FOR ENERGY EFFICIENT TRUST SYSTEMS IN WSNS

*Sakthi Priyanka. V [1], Dr. Jeen Marseline K.S[2]*

## Abstract

The technique of using watchdog is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). Watchdog technique is used to identify and monitor the malicious node in network. This technique is also used for trust behavior collection, hence gets a very good performance in guarding data sensing and multi-hop routing. It is proved as a very effective approach to build up WSNTS's foundations. However, this kind of technique requires much energy and hence decreases the lifespan of WSN.The inefficient use of watchdog implementation in existing trust systems lead me to propose an optimization method for energy consumption of watchdog and making it dynamic, while keeping a sufficient level system security. In the proposed method dynamic watchdog optimization method is used. DBP algorithm is used and AODV protocol is used for dynamic routing. Through which a considerable amount of energy is saved. To optimize watchdog frequency and to calculate the energy consumed by each node HWFA (Heuristic Watchdog Frequency Adjustment Algorithm) is used. Replacement or recharging of those sensor node's power is very expensive and difficult. More precisely, sensor nodes are usually equipped with limited energy and they have to work for a long period in various isolated terrains. In the proposed method optimization of the watchdog location is done using DBP algorithm. The dynamic watchdog optimization can improve the efficiency in a significant manner throughout the Wireless Sensor Network and energy required can also be optimized through HWFA. This is done with NS2 in windows OS and the output is simulated to analyses the Performance.

*Index Terms : WSN,Security,Trust System,Energy-Efficient,Watchdog Technique.*

## I. Introduction

Wireless Sensor Networks have been used in challenging, hostile environments for various applications such as forest fire detection, battlefield surveillance, habitat monitoring, etc. Sensing, computation and communication is done by tiny piece of electronic devices in wireless sensor networks. One common assumption in traditional Wireless Sensor Networks is that a trusted third party, e.g., a sink, is always available to collect sensed data in a near-to-real-time fashion. Although many Wireless Sensor Networks operate in such a mode, there are WSN applications that do not fit into the real time

[1] Research Scholar, Department of Computer Science, Sri Krishna Arts and Science College.

[2] HOD Department of IT, Sri Krishna Arts and College.

data collection scenario[4-12].A Wireless Sensor Network comprises of battery-powered sensor nodes with extremely limited processing capabilities. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multihop path. However, the multihop routing of Wireless Sensor Networks often becomes the target of malicious attacks. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference[4][19][23-24]. The WSN is built of few nodes to several hundreds or even thousands of nodes, where each node is connected to one (or sometimes several) sensors. A critical complement to security mechanisms such as cryptographic methods, authentication and access control logics etc[1][2][3].

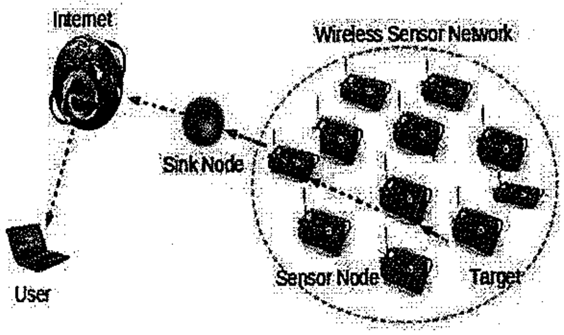


**Figure 1.1 WSN Network**

These trust systems are widely applied to protect wireless sensor networks from being attacked by trust sensor node. Those nodes can bypass traditional security protections using their trust identities, but can't be captured by trust systems due to their poor reputation or past misbehavior[13].However, collecting enough past behaviors through business traffic, to build are liable trust system for WSN is not a trivial task. The problems which are found while building these trust systems are. First, sensor nodes may not be located in the communication range for base station or cluster head. Second, some sensor node may not be communicating with other nodes or it may be communicating with low frequency. Third, the information obtained from one sensor node cannot be used to build trust system for other sensor nodes[14][15].

Although the watchdog technique has been proved as a very effective approach to build up Wireless Sensor Network Trust System foundations, it introduces a large amount of additional energy which conflict the energy efficient design principle of Wireless Sensor Networks. Recharging or replacement of nodes power is very difficult and expensive. Due to those challenges, energy saving plays a very important role in the design of modern Wireless Sensor Networks. In particular, some Wireless Sensor Network Trust Systems do not discuss how to schedule watchdogs in their proposals, while some other simply suggest letting sensor nodes launch neighbor flooding watchdog tasks to monitor all their neighbors and do not study which frequency is appropriate for their monitoring[4][6][20].This watchdog technique requires much energy, Thereby network life time is decreased.

### *Watchdog Optimization*

Two ultimate goals when optimizing watchdog techniques: First is to minimize the energy usage of the whole WSN and the other is to maximize the security (in terms of trust accuracy and trust robustness). The optimization goals as follows: Minimize the energy required throughout the whole WSN and maximize trust accuracy of WSN. Hence the Watchdog Optimization is the core area of energy optimization.

The watchdog technique is a trust based intrusion detection technique which identifies the malicious nodes and its activity in the network is to monitor the nodes within its communication range. The nodes selected as the watchdog nodes are the most trustworthy nodes due to its inherent features like, highly stable[6][16][17]. These watchdog nodes are deployed in the network randomly just as any other node. When any node transmits its data packets towards its destination node through the intermediate nodes, the watchdog present within the communication range of the transmitting node and also the intermediate node, can determine whether the data packet is being properly transmitted by the intermediate node. Thus the watchdog node checking the validity of the nodes is involved in the transmission of the data packet. The goal of this project is to reduce the energy cost induced by watchdog tasks as much as possible, while keeping robustness and trust accuracy in a sufficient level. To touch this goal, we can optimize the technique of implementing watchdog in two levels.

At First the watchdog locations are optimized by considering the fact that, the sensor nodes which are located closely may require less energy and to monitor each other due to shorter communication distance between them. So these nodes are more likely of being compromised themselves and cause collaborative attacks. Therefore explore the optimal watchdog location to minimize the overall risk (in terms of both security and energy consumption).

Second, the watchdog frequency is optimized and reduce its redundancy. The watchdog frequency and redundancy optimization using HWFA can reduce the energy required and increase the efficiency of the whole system of WSN.

This technique is used to dynamically create shortest path between intermediate nodes to target node. For the Optimization of Watchdog Location, the DBP algorithm is used, to find the minimum location distance of the target node. Here the routing is based on AODV protocol. This algorithm is used to calculate the routing path. All the active nodes in WSN, Once the correct destination is found, an end-to-end connection is established to carry end-system. This connection remains active as long as the file requested transferred and it is dynamically shut down when not in use. Here the mobile sink node temporarily assigns watch dog for every data transfer, this will avoid delay and waiting time. The allocation of watch dog entirely depends on the distance between the source and destination nodes. Once the node will be assigned as watch dog node, the node will protect the packets from unauthorized access until the process get over. After the successful packet transfer the watch dog node will become normal node.

The main objectives of this paper are

- To reduce energy required by the sensor nodes by optimizing watchdog locations.
- By optimizing network lifetime can be increased.
- Maintaining the security in sufficient level.
- Dynamic watchdog assignment.

## II. Existing Method

WSN provide a wide variety of business traffic to build up all kinds of trust. To tackle those challenges and facilitate past behavior collection, most of existing WSNTSs have adopted a watchdog technique. This technique allocate the watchdog task to the node, to monitor its neighbor node at time slot. A watchdog task consists of a bidirectional communication between the watchdog node and the target node. But this technique required large amount of energy. The inefficient use of watchdog technique in existing trust systems decreases energy consumption in WSNTs. sensor nodes are usually equipped with limited battery, and work in an unattended mode for a long period of time to adapt various harsh environments such as the deep desert and ocean abyss. Due to those challenges, energy saving plays a very important role in sthe design of modern WSNs. Existing WSNTSs dont gives appropriate solutions to save the energy consumption problem. And also some WSNTSs do not discuss how to schedule watchdogs.The trust-energy conflict induced by watchdog usage has not been addressed before.

In particular, some WSNTSs do not discuss how to schedule watchdogs in their proposals, while some others implicitly suggest letting sensor nodes launch neighbour-flooding watchdog tasks to monitor all their neighbors and do not study which frequency is appropriate for their monitoring.

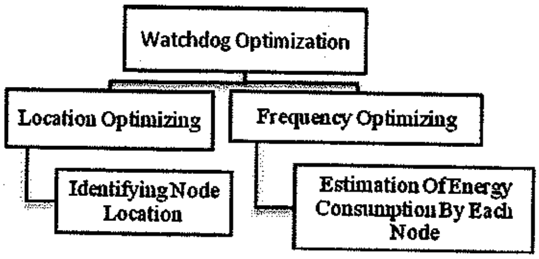
### *Disadvantages of existing method*

1. This kind of technique requires much energy.
2. They do not give appropriate solution for energy consumption problem.
3. This technique do not efficiently identify and blocks the attacking nodes.
4. Decrease the network lifetime.

## III. Proposed Method

To overcome trust-energy problem, propose the dynamic watchdog optimization technique for WSNTSs. This technique is used to balance energy efficiency and security in terms of trust accuracy and robustness. While sending information from source to destination, in the path there will be many intermediate nodes. In this dynamic watchdog optimization method ,the neighbor or nearest node will be changed as the watchdog node for the purpose of reducing the energy requirement. This watchdog is called as a dynamic watchdog. And also the watchdog frequency is optimized. Ultimate goal is to reduce the energy cost induced by watchdog tasks as much as possible, while keeping trust accuracy and robustness in a sufficient level. For dynamic routing AODV (Adhoc On Demand Distance

Vector)routing protocol is used. And to touch this goal, watchdog technique is optimized in two levels.


Watchdog Optimization
Location Optimizing
Frequency Optimizing
Identifying Node Location
Estimation Of Energy Consumption By Each Node

**Levels of watchdog optimization Technique**

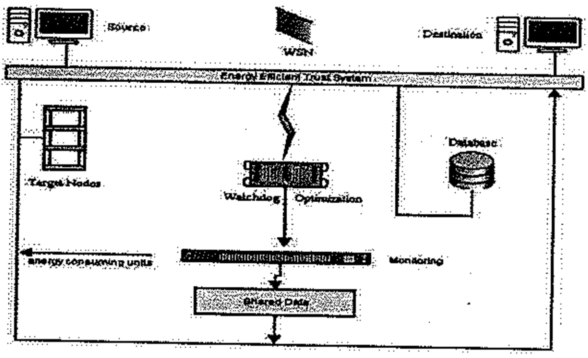
First level to optimize watchdog locations, given a target node to minimize the overall risk in terms of both energy consumption and security. Watchdog Location Optimization technique using DBP (Distance Based Probabilistic) algorithm to identify the nearst node for watchdog and create shortest distance communication. It identify the misbehaving sensor nodes and prevents those nodes from being used for future routing. So proposed an energy efficient secure routing algorithm to choose efficient and trustworthy next-hop node in a route.

Second level to optimize watchdog frequency and reduce its redundancy. Watchdog Frequency Optimization technique using HWFA (Heuristic Watchdog Frequency Adjustment) algorithm to estimate energy units for each node. Based on this energy unit the node transfer the data to intermediate nodes. This algorithm define the number of watchdog tasks taken by watchdog node to monitor a target node within a time window as watchdog frequency. Also, define a node's behavior frequency and attacking frequency within the time window.

***Benefits of Proposed Method***

- This technique efficiently saves the energy.
- Watchdog location optimization.
- Watchdog optimization to minimize the energy cost of watchdog usage.
- This method saves the nodes energy so it increases the network lifetime and trust accuracy.
- Dynamic assignment of Watchdogs.

comparison with the existing system design. All the inputs entered are completely raw, initially, before entering into a database, then each of them available processing.



**Architecture diagram of watchdog optimization in WSN**

## IV. Methodology

### *1.Threat Model*

*The different security concerns of Wireless Sensor Network are as follows:*

1. Data Confidentiality: It means the content of the message when transmitted across the network must remain confidential i.e. only the intended receiver and no one else should be

able to read the message. Hence encryption is used for effective and secure communication in which data is encrypted into secret words.

2. Data Integrity: It means data must reach the destination without being changed by the adversaries or Attackers. Data Integrity ensures that the data has not been changed during the transmission, neither accidentally or intentionally. Checksum is used for data integrity.

3. Data Authentication: It is the fundamental requirement for security in WSN. Attacks in the sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets. In message authentication, receiver needs to be sure of the sender's identity as an adversary can change the entire data. So the receiver needs to be assured that whatever data used in Decision making process comes from an authorized source or not.

4. Data Freshness: Data freshness ensures that data should be recent and no old messages have been replayed. This requirement is essential when shared key strategies are used. So there is a great need to get renew the shared keys time to time. As it takes a little bit time to propagate the shared keys over the entire network during that time adversary can perform a replay attack. To tackle the problem of the replay attack timestamp is added to the message.

By exploiting the "legitimate" sensor nodes, attackers could perform insider attacks to disrupt WSN's normal functionalities, such as damaging the quality of multihop routing by selectively dropping routing packets or misleading WSN's data aggregation by reporting crafted sensing data. Those attacks can avoid traditional security mechanism Moreover, we consider attackers smart enough and are aware of the existence of WSNTS. Those attackers attempt to evade WSNTS's detection by launching some advanced attacks. In particular, we consider four types of WSNTS attacks in this paper. The first is an on-off attack, where attacker's node may behave well for a long time to get enough reputation then do malicious behaviors suddenly. The second is a discrimination attack where attacker's node will behave differently to different sensor nodes (watchdogs). The third is a bad-mouthing attack, where attacker's node will perform watchdog tasks and report an honest node as a malicious one. The last is a Sybil attack where attackers can control a large number of sensor nodes to mislead WSNTS.

### *2.Trust Model*

Intermediate nodes computing or networking is a distributed application that partitions watchdog's task between source and target nodes. These nodes are connected and communication is done using IP address and host name. Often Inheritor nodes operate over a network on separate functionalities. A server machine is a high performance host that is running one or more tasks which share its resources with nodes. Three concepts are introduced here. One is trustworthiness that can be used to estimate a sensor node's behavior. The other two are trust accuracy and trust robustness, which can be used to measure how accurate the target nodes' trustworthiness can be recovered in the presence of WSN attacks and WSNTS attacks respectively. Unlike the trustworthiness that the trust systems need to calculate at run time, the trust accuracy and trust robustness are two performance indices that we can use to evaluate and compare different trust systems' security levels. Trust systems do not need to compute the trust accuracy and robustness at run time

### *Trustworthiness*

A monitoring mechanism known as watchdog to identify misbehaving nodes in wireless ad hoc networks. In their approach, each sensor node has its own watchdog that monitors and records its one hop neighbors' behaviors such as packet transmission. When a sending node S sends a packet to its neighbor node T, the watchdog in S verifies whether T forwards the packet toward the S or not by using the sensor's overhearing ability within its transceiver range.But for routing task, watchdog nodes expect target nodes can successfully help forward packets. Tij is calculated as :

$$T_{ij} = \frac{\sum t \in NV\, \omega_{ij}^{t} \neq \emptyset I_{ij}^{t}}{\sum t \in NV\, \omega_{ij}^{t} \neq \emptyset 1}$$

### *Trust Mechanism*

In general, trust mechanism works in the following stages.

1) Node behavior monitoring: Each sensor node monitors and records its neighbors' behaviors such as packet forwarding. The confidence of the trustworthiness evaluation depends on how much data a sensor collects and how reliable such data is.

2) Trust measurement: Trust model defines how to measure the trustworthiness of a sensor node. Several representative approaches to build the trust model, which include Bayesian approach, Entropy approach, Game-theoretic approach, and Fuzzy approach.

$$T = \frac{s+1}{s+f+1}$$

3) Inside attack detection: Based on the trust value, a sensor node determines whether its neighbor is trustworthy for collaboration (such as packet forwarding). as an untrusted or malicious node. Depending on the WSN's trust mechanism, the detection of such insider attacker may or may not be broadcast to the rest of the nodes in the WSN.

### *Trust Accuracy*

We let $I_t^j$ be the event to describe a sensor node $v_j$'s internal behavior and draw it according to a binary distribution function Pj . = 1 if vj behaves well at time slot t while = 0 if performs attacks against WSN at t (e.g., reporting corrupted sensing data or refusing packet forwarding etc.). Watchdog node can sample Pj to discrete events . We then model the accuracy of Tij (i.e., trust accuracy) using the Kullback-Leibler divergence between the probability distribution of s (i.e., Pj) and the distribution of s (denoted as Qij ). KL divergence is a well known measure of the information loss when using one information source (i.e., probability distribution) to approximate another, and hence being a good choice to measure trust accuracy. Let I be the random variable of distribution Pj and Qi j . We then can follow to calculate KL divergence as :

$$D_{KL}(P_j \parallel Q_{ij}) = \sum_I \ln\left(\frac{P_j(I)}{Q_{ij}(I)}\right) P_j(I)$$

We use $\Delta_{ij}$ to denote trust accuracy and measure it as:

$$\Delta_{ij} = \frac{1}{D_{KL}(P_j \parallel Q_{ij}) + 1}$$

### *Trust Robustness*

Traditionally, trust is estimated based on the observed weight of misbehavior. In order to record and manage observations, we use a time-window mechanism. According, node x records observations about node y, in which Sx,y and Ux,y are the numbers of good and bad behaviors, respectively, of node y as observed by node x. Moreover, the time window consists of three time units, L = 3. After each Δ time period, the time window slides to the right, adding a new time unit and deleting the very first time unit.

Based on the rate of misbehavior in each time unit, node x estimates the weight of misbehavior as follows:

$$W_j = \max\left(\alpha_1 r_1, \alpha_2 r_2, \ldots\ldots, \alpha_j r_j, \alpha_L r_L\right)$$

By considering WSNTS attacks, a target node vj's behavior is observed by different watchdog nodes are likely different. For example, some malicious target nodes may behave differently to different watchdog nodes (discrimination attack), and some malicious watchdog nodes may report false observations to others (bad-mouthing attack). To address this issue and enable our analysis to cover WSNTS attacks, a new concept trust robustness is introduced, to measure WSNTS's effectiveness against WSNTS attacks. It is defined as mean value of trust accuracy provided by a group of cooperative watchdog nodes. This definition can naturally bound the average effectiveness of watchdog nodes in the presence of the WSNTS attacking model. Let Òj be the trust robustness of target node vj.

$$\square j = \frac{\sum v_i \in W_j \Delta_{ij}}{\|W_j\|}$$

### 3.*Target Nodes and BlackHole Detection*

Choose the target node from the intermediate nodes. Then the number of connections between each pair to target node is established between each and every nodes for network communication. From the source node to the destination node and intermediate nodes, must have connection between source nodes, after communication between combinations of multiple nodes each and every node must have link to each other. To choose the neighbour nodes and to communicate with each other, set the priority queue in the network communications.

We use **AODV** protocol as the routing protocol in this method.

Neighbor set is defined as, all the nodes that are within the radio transmission range of a node.Due to the rapid moment of the nodes, the neighbor set of a node keeps changing and it is expected that the neighbor set changes faster when mobility increases. The chance that two mobile nodes have the same neighbor set at the same time is very small. So the neighbor set provides a good "identity" of a node, i.e., if the two neighbor sets received at the same time are different enough,it is concluded that they are generated by two different nodes.

Two processes are implemented to say that determining neighbor set of a node is a good identification for finding malicious node.

- In the first experiment, we measured the neighbor set difference of one node at different time instants *t* and *t* + *I* under different moving speeds and system size (i.e., number of nodes in the system), where *I* means one second.
- In the second experiment, we examined the neighbor set difference of two different nodes, say node A and node B, at the same time. We measured the number of Nodes in the set of *(({A's neighbor set} U {B's neighbor set})-({A's neighbor set} )" {B's neighbor set})).*

Based on this neighbor set information, we design a method to deal with the black hole attack, which consists of two parts: **detection and response.**

In order to collect neighbor set information, we introduce two types of control packets in the detection phase : *requestneighborset*(RQNS) and *replyneighborset*(RPNS).

- The packet format of RQNS is as follows:

{*srcaddr. destaddr. requestneighborseq#, nexthop* }.

srcaddr is the IP address of the source node S

destaddr is the IP address of the destination D.

- Each node is responsible for maintaining one counter: the sequence number of the RQNS, Each time a node sends a RQNS, requestneighborseq# increases by one. The sequence number in each node uniquely identifies the RQNS, which unicasts to the destination using the underlying AODV routing protocol.

- D or D' (malicious node), after receiving RQNS, replies

a message RPNS.

- The message format of RPNS is as follows: ***{srcaddr, destadd, requestneighborseq#. neighbor set}***

The first three items, i.e., *srcaddr, destaddr, requestneighborseq#,* identify to which RQNS this RPNS corresponds.Neighbor set contains the current neighbor set of D or D'.This RPNS unicast back to S.

### *BLACK HOLE DETECTION*

**Step 1: Collect neighbor set information.**

By using AODV protocol, the source node S floods RREQ packets across the network to find a route to the destination node D. Now for each received RREP, S will unicast a RQNS packet, and the RQNS packet will go to either D or D', depending on the path contained in RREP.After D or D' receives RQNS, it will generate a RPNS packet, which contains its current neighbor set, and unicast it back to S.

**Step 2: Determine whether there exists a black hole attack.**

The source node S, after receiving more than one RPNS packet in a certain period will start comparing the received neighbor sets. The difference among the neighbor sets is defined as the union of the received neighbor sets minus the intersection of the neighbor sets. If the difference is larger than the predefined threshold value, S will know that the current network has black hole attacks and take some actions to respond to it. One concern is that what if D' first requests the neighbor set of D, and replies it to S? We think that it is difficult for D' to do so. Because D' claim D's address, D' has to use D's address to request D's neighbor set, (otherwise, D's neighbors can find that D' is a masquerader). But D will raise an alert to this request, because it uses the same address of D.

### RESPONSE

We assume there exists a public key infrastructure, which S can use to authenticate D or D'. After S detects the black hole attack, it will use the cryptography-based method to authenticate D and D'. In this way, S can identify D, the true destination.Once D is identified, S will send a *modifyrouteentry* control packet to D to form a correct path by modifying the routing entries of the intermediate nodes from S to D. We call this routing recovery protocol. The packet format of MRE is as follows:***{destaddr, correctpath }***

*destaddr* is the IP address of D. *correctpath* is the hop by hop path from S to D. S can get the information *correctpath* from the received RPNS's. After each node receives the MRE,it will modify its corresponding routing entry (identified by the IP address of D) to make its next hop on the path to D, instead of D'. After D receives MRE, a correct path has formed between S and D, which will make the traffic of S go to the correct destination.

### *4.Dynamic Watchdog Location Optimization*

This technique is used to create shortest path between intermediate nodes to target node dynamically. Watchdog Location Optimization is to identify the nodes location. DBP algorithm is used to find the minimum location distance of the target node. Based on Adhoc On Demand Vector Routing Protocol routing between nodes is designed.All the active nodes in WSN, Once the correct destination router is found, an end-to-end connection is established to carry end-system. This connection remains active as long as the file requested transferred and it is dynamically shut down when not in use.

To optimize the location of watchdog, Have to find the optimal Wj , "v j " V by directly solving the optimization problem described because they are ill-posed and do not have solution in closed form. To conquer this challenge, we find optimal watchdog positions instead (find optimal dij given "vj " V). The selection of neighbor nodes vi " Bj which are located near to the optimal dij is more likely able to form the optimal Wj.

To transform the original optimization problem of finding optimal Wj to the problem of finding optimal dij, the intuitive evidence is that, although the vi " Bj with a less dij requires less energy to perform watchdog tasks to monitor vj and hence ensure the energy minimization goal in such vi is more likely controlled by attackers if vj is an attacker's node. The use of attacker's node as watchdogs will impede the security maximization goal in since those sensor nodes can report fake watchdog results to drop the trust robustness.so find the optimal watchdog location dij given a target node vj by considering an overall risk(which considers both energy and security).For all sensor nodes, we cannot assume there necessarily exist some neighbor nodes located at the optimal watchdog location. In common, vj " V may have their neighbors. To address this issue, an intuitive solution is to choose the node nearest to the optimal location as watchdog. That is, it fixes the watchdog node to vj's nearest neighbor, vj " A can simply behave well to vj's nearest node.

### *5.Energy Consumption*

The algorithm proposed here is HWFA (heuristic watchdog frequency adjustment) algorithm. In the HWFA algorithm, watchdog frequency is adjusted adoptively by referencing trust worthiness.An energy-efficient trust model by applying geographic target nodes to identify trust managers (may save energy due to low storage usage), an energy watcher is implemented to help sensor nodes for estimating their neighbor node's energy cost for each packet forwarding. Thus it enables the selection of the most efficient node as their next hop in the route. Watchdog Frequency Optimization technique is used to estimate energy consumption of each nodes. Energy watcher uses the HWFA algorithm to calculate energy value of each nodes. Depending on this value the files are transfer to the target node.

In this model, a sensor node's transmitter unit to the main node as file request sends data to multiple requested node. DBP algorithm used here avoids the WSNTS attacks. The source node sends all type of file, and then enters the data send from source node to destination node over the network. As well as data must be send from source node to intermediate node automatically in this module. The data's are successfully transfer from source to destination without attacks. watchdog frequency is adjusted adoptively by referencing trust worthiness. The watchdog frequency should increase when the trust worthiness grows up from 0 to 0.5 but decrease when it climbs from 0.5 to 1, and the other is that the smallest should not be 0.

***Design goals :***

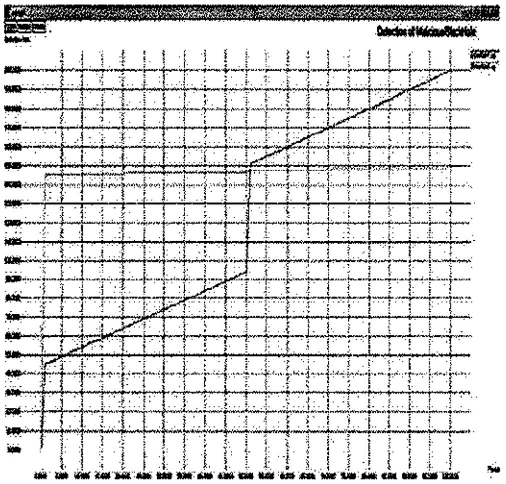
1. The first design goal is to ensure that the watchdog frequency is high if the target node is uncertain but low if the target is determined.
2. The second design goal is to guarantee that the watchdog node never disables the monitoring to the target node at any time.

Heuristic Watchdog Frequency Adjustment Algorithm(HWFA) orders nodes by their priorities, breaking ties by distance. They are estimated as follows: For each node ni, we define its release time ri as the last time Ti's freshness delta changed from zero to nonzero (i.e., the last arrival of new data in case of base tables, or, for derived tables, the last movement of the trailing edge point of its source tables). Then the distance of Ji to be RI þ Pi (recall that the period of a derived table is the maximum of the periods of its descendants) is estimated.

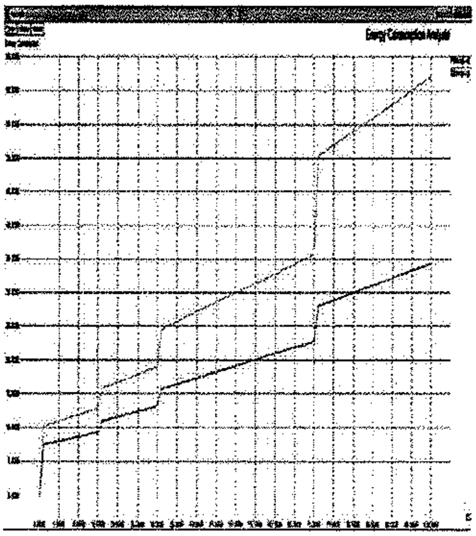
$$\textit{Energy saving} = \frac{\textit{cost (Baseline)} - \textit{cost (WO)}}{\textit{cost (Baseline)}}$$

## V. Experimental Results

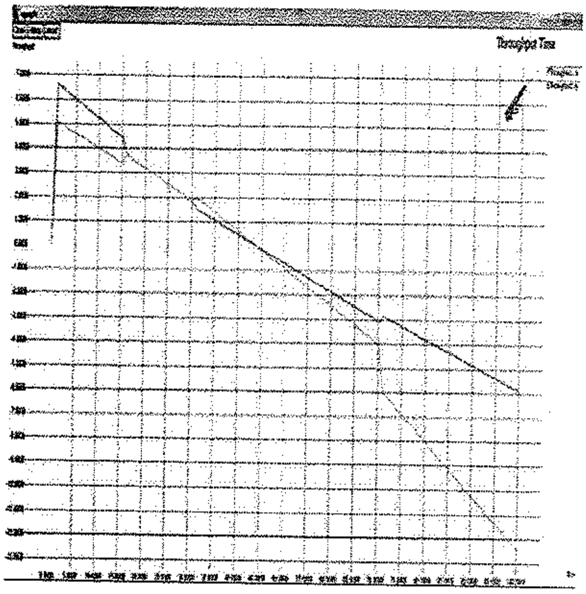
The Performance will be analyzed by the following graphs



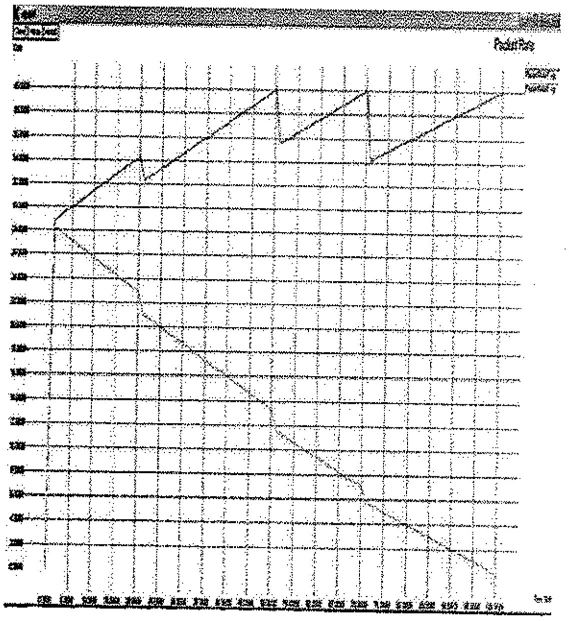
**Graph-1 Node Detection**



**Graph-2 Energy Optimization Using Watchdog**



Graph-3 Throughput Topology



Graph-4 Rate of Delivered Packet Data

### *Simulation Setup*

WSNET is an event driven module based WSN simulation framework. Start with sender. The sender sends Hello packets for all the nodes in the network to check whether all the nodes are an activation or not. Incase if some nodes are does not in activation, then it activate that node. For example, let assume one sender with two receiver sender, receiver respectively. Denotes node's position. Then we define routed path using topology formation. After that, packet will be transformed to node by node. Some nodes are forwards the packets to another node but few nodes are does not forward the packets to another node. It is called malicious node.

### *Node Creation*

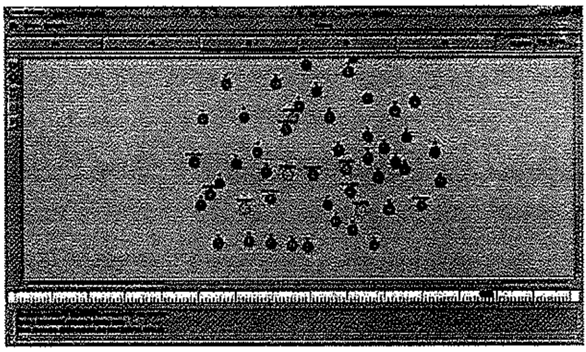
This module is developed to node creation and more than 30 nodes placed particular distance. Wireless node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

### *Node Configuration Setting*

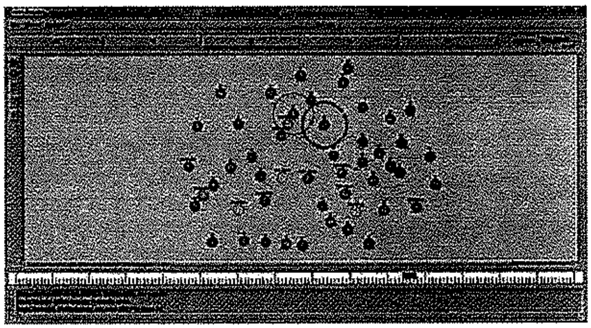
The sensor nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes. Fix the configuration to all of the nodes in communication network.

### *Detecting Trust Node*

Detection of trust node should takes place using watchdog. The node which detect this, should forward this information to source node.



*Simulation for Attacker Node*



*Simulation for Dynamic Watchdog Optimization*

**Performance Metrics**

*Comparison of Existing with proposed system*

| Metrics | Existing | Proposed |
|---|---|---|
| Throughput (%) | 69 | 92 |
| Detection time (%) | 82 | 95 |
| Energy consumption (%) | 86 | 78 |
| Packet transfer rate (%) | 90 | 96 |

## VI. Future Enhancement

In future whenever the network demands more efficient system for wireless sensor networks, then the watchdog efficiency can further improved by increasing the energy consumption and the speed of action or increased security implementation within the clustered topology of sensor nodes. The higher levels of algorithms are to be developed for achieving those objectives. However the watchdog can remain as the trust system element within the networking of sensors. The Wireless sensor networks will remain as our future communication links in various higher modes of operations even in our space exploration or in secret military operations etc.The Dynamic watchdog optimizing technique can also be applied to vehicular ad-hoc network and all other networks which are similar to wireless sensor network.

## VII. Conclusion

In this proposed work, Watchdog Optimization algorithm is presented by considering a new approach to save more energy and make it dynamic keeping the security in sufficient level in Wireless Sensor Networks. It can be used to solve several optimal problems. It is aimed to minimize the length of the tour to find the target path. Algorithm is highly flexible and can be effectively used to find shortest path by considering very few control parameters as compared with the other heuristic algorithms dynamically. This gives a promising research direction on the design of energy-efficient WSNTS by optimizing the collection procedure of first-hand experiences.

## References

[1] A. Perrig, J. Stankovic, and D. Wagner, *"Security in wireless sensor networks," Commun. ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[2] M. L. Das, *"Two-factor user authentication in wsn," IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar.2009.

[3] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wsn," *Ad Hoc Netw.*,vol. 5, no. 1, pp.3–13, 2007.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, *"Mitigating routing misbehavior in mobile ad hoc networks,"* in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, 2000, pp. 255–265.

[5] E. Shi and A. Perrig, *"Designing secure sensor networks," IEEE Wireless Commun.*, vol. 11, no. 6, pp. 38–43, Dec. 2004.

[6] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, *"Reputation-based framework for high integrity sensor networks," ACM Trans. Sensor Netw.*, vol. 4, no. 3, 2008, Art. ID 15.

[7] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, *"Group-based trust management scheme for clustered wireless sensor networks," IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[8] G. Zhan, W. Shi, and J. Deng, *"Design & implementation of TARF A trust-aware routing framework for WSNs," IEEE Trans. DependableSecure Comput.*, vol. 9, no. 2, pp. 184–197, Mar./Apr. 2012.

[9] S. Zheng and J. S. Baras, *"Trust-assisted anomaly detection and localization in wireless sensor networks,"* in *Proc. 8th Annu. IEEE Commun.Soc. Conf. Sensor, Mesh, Ad Hoc Commun., Netw. (SECON)*, Jun. 2011, pp. 386–394.

[10] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, *"A novel approach to trust management in unattended wireless sensor networks," IEEE Trans. Mobile Comput.*, vol. 13, no. 7, pp. 1409–1423, Jul. 2014.

[11] X. Li, F. Zhou, and J. Du, *"LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 924–935, Jun. 2013.

[12] D. Wang, T. Muller, Y. Liu, and J. Zhang, *"Towards robust and effective trust management for security: A survey,"* in *Proc. 13th IEEE Int. Conf. Trust, Secur., Privacy Comput. Commun. (TrustCom)*, 2014.

[13] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, *"A survey of trust and reputation management systems in wireless communications," Proc.IEEE*, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.

[14] F. G. Nakamura, F. P. Quintão, G. C. Menezes, and G. R. Mateus, *"An optimal node scheduling for flat wireless sensor networks,"* in *Proc. 4th Int. Conf. Netw.*, 2005, pp. 475–482.

[15] A. Salhieh, J. Weinmann, M. Kochhal, and L. Schwiebert, *"Power efficient topologies for wireless sensor networks,"* in *Proc. Int. Conf. Parallel Process.*, Sep. 2001, pp. 156–163.

[16] J.-H. Cho, A. Swami, and R. Chen, *"A survey on trust management for mobile ad hoc networks," IEEE Commun. Surv. Tuts.*, vol. 13, no. 4,pp. 562–583, Oct./Dec. 2011.

[17] Y. Yu, K. Li, W. Zhou, and P. Li, *"Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, 2012.

[18] X. Chen, K. Makki, K. Yen, and N. Pissinou, *"Sensor network security: A survey," IEEE Commun. Surv. Tuts.*, vol. 11, no. 2, pp. 52–73,Apr./Jun. 2009.

[19] R. Yan, H. Sun, and Y. Qian, *"Energy-aware sensor node design with its application in wireless sensor networks," IEEE Trans. Instrum. Meas.*, vol. 62, no. 5, pp. 1183–1191, May 2013.

[20] P. Michiardi and R. Molva, *"Core: A collaborative reputation mechanismto enforce node cooperation in mobile ad hoc networks,"* in *Proc. IFIP TC6/TC11 6th Joint Working Conf. Commun. Multimedia Secur., Adv. Commun. Multimedia Secur.*, 2002, pp. 107–121.

[21] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensornetworks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, Oct. 2002.

[22] R. Di Pietro, G. Oligeri, C. Soriente, and G. Tsudik, "United we stand: Intrusion resilience in mobile unattended WSNs," *IEEE Trans. Mobile Comput.*, vol. 12, no. 7, pp. 1456–1468, Jul. 2013.

[23] F. Bao, I. R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust based routing and intrusion detection," *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.

[24] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: A trust-aware secure routing framework in wsn," *Int. J. Distrib. Sensor Netw.*, vol. 2, Jan. 2014, Art. ID 209436.

## Author's Biography

**Sakthi Priyanka Venugopal** is currently a Research fellow with Sri Krishna Arts and Science college, Coimbatore. She received the Msc in Computer Science from Sri Krishna Arts and Science College,Coimbatore.Her research interests include Wireless Sensor Networks and Artificial Intelligence.

**Dr. K.S.Jeen Marseline,** M.C.A., M.Phil., Ph.D., she is currently the Head of the department of Information Technology with Sri Krishna Arts and Science College, coimbatore. She received Ph.D degree in Image Processing from Bharathiar University, Coimbatore.She has 18 years of teaching experience. Her research interests are Data Mining and Image Processing.