Enhancing Wireless Sensor Network Security using Artificial Neural Network based Trust Model

Dr. Adwan Yasin[1]
Dept. Engineering and Information Technology
Arab American University
Jenin, Palestine

Kefaya Sabaneh[2]
Dept. Engineering and Information Technology
Arab American University
Jenin, Palestine

***Abstract*—Wireless sensor network (WSN) is widely used in environmental conditions where the systems depend on sensing and monitoring approach. Water pollution monitoring system depends on a network of wireless sensing nodes which communicate together depending on a specific topological order. The nodes distributed in a harsh environment to detect the polluted zones within the WSN range based on the sensed data. WSN exposes several malicious attacks as a consequence of its presence in such open environment, so additional techniques are needed alongside with the existing cryptography approach. In this paper an enhanced trust model based on the use of radial base artificial neural network (RBANN) is presented to predict the future behavior of each node based on its weighted direct and indirect behaviors, in order to provide a comprehensive trust model that helps to detect and eliminate malicious nodes within the WSN. The proposed model considered the limited power, storage and processing capabilities of the system.**

***Keywords*—Wireless sensor network; security; Artificial neural network; trust rate; malicious node; trust model; threat**

I. INTRODUCTION

Wireless sensor network is a distributed system that contains a collection of autonomous spatially distributed nodes cooperating together to produce a globally useful information from its local raw sensed data. WSN introduced significant advantages upon traditional communication technologies in many fields such as healthcare applications which could be wearable or even implemented in the patient body, transportation, military operations and environmental conditions monitoring like fire and natural disaster detection.

WSN node contains a set of components; one sensor or more to sense the environmental conditions as the concentration of a specific chemical element in our case, a small processing unit, storage and a power supply (battery). Each of these components have to be used in a rational way since the resources of the node are limited and it is difficult or even impossible to fed or replace it [1] [2].

Wireless sensor network may contain tens, hundreds or even thousands of autonomous nodes equipped with sensors. It is essential to choose a suitable network topology that enables the communication between several nodes, and the transmission of sensed data. The main driving factor in selecting which topology should be used is the limited power supply within WSN nodes, and also the need to reduce the price as much as possible because hundreds of nodes should be connected and interact. It is possible to use the bus topology, ring, star, mesh, tree or hybrid topology. A hybrid topology that combines star, mesh and ring topologies together is proposed to provide a reliable, fault tolerant and power efficient communication and data transmission [3].

Using WSN in water pollution monitoring requires the existence of sensing nodes in a harsh and changeable environment, that makes it exposed to several security threats and dangers. A sensing node could be damaged due to environmental changes and conditions, also it may be a target for an opponent party and simply be replaced or even modified in such a way that facilitates a passive or active attack by the opponent. As a result preserving the system security is an important and essential issue to prevent any unauthorized access to its components. Several techniques are used such as symmetric encryption, it depends on the use of a single key in both sides sender node and receiver one, but such methodology is not enough and we need an additional strategy that distinguish a malicious node even if it somehow obtained the key. Building trust between the different nodes is the intended approach [4].

Building trust between system nodes requires the use of a trust model to provide trust ratings for WSN sensor nodes depending on their performance and sensed data, higher the trust ratings for a specific node higher its effectiveness, while lower the trust rate means higher probability to remove it from the system especially when it becomes lower than a specific threshold [5].

Several trust schemes had been used to discover the malicious nodes in WSN, all of them are based on two essential characteristics in terms of WSN resources limitations; in one hand they are lightweight and need less power, processing and communications, in the other hand they are powerful and capable of managing trust between various heterogeneous nodes [6].The proposed trust model aims to enhance the use of artificial neural network(ANN) in WSN using radial basis function benefiting from its simplicity in implementation to provide a comprehensive trust model that supports system security and rationalizes resources consumption.

The rest of the paper is ordered as the following; in section II a literature review that lists the state-of-the-art security approaches and trust models, while section III proposes a comprehensive architecture for the WSN system including system components and the network topology. In section IV securing the WSN is discussed, while section V focuses on

how to build trust between several nodes in WSN using ANN, VI includes a proposed enhanced trust model. Finally section VII concludes with the future work.

II. Literature Review

The raised popularity of WSN had been facing several security threats and permutations. Developing corresponding countermeasure mechanisms suffered from challenges represented by the sensors size, processing power and memory limitations. Data within a water pollution monitoring system should be protected from any unauthorized party since water is the basic resource of life for all countries, so security mechanisms are essential to perceive confidentiality, availability and integrity of the WSN components including hardware devices, software, networking equipments and collected data [7].

Attacks in WSN are categorized to two main approaches; either attacks against the employed security mechanism or attacks against the routing mechanism. An attack that aims to hack the security mechanism by exploiting its weaknesses depends on the mechanism characteristics while the last depends on hacking the routing algorithms within the network [8] [12].

Denial of service attack (DoS) prevents the normal use of the communication facilities within the network by exhausting its resources with extra transmitted packets; it aims to flood the network with useless data and may eventually disrupt the whole network [5]. Sybil attack is another threat in which a node claims numerous identities so it behalf and interact as a set of legitimate nodes, data integrity and resource utilization degrades and as a result network protocols may be disrupted [11]. In black whole attack a malicious node attempts to track and attract the traffic in the network, once the opponent can access, communicate and participate in the network the entire readings could be affected especially in the hierarchal network topologies where data is transmitted passing through several nodes. Hello flood attack is incorporated by a foreign adversary who can flood hello request to any legitimate node in the network and break the security mechanism, while in wormhole attack the attacker record the packets and forward to another location, one or more fake nodes are used with a route between them, once the malicious node starts its work a fake route is used to provide a path that is shorter than the original one, and as a result the data is tunneled within the undesirable route [9].

Basically WSN defensive line depends on the use of conventional key approaches for intrusion detection and prevention, symmetric encryption techniques help to hide the content of transmitted packets through the network such that no malicious node can make use of encrypted data even if it get the ciphered packets, and this is distinguished by its reduced overhead compared with public encryption algorithms. The network is still facing the previous types of attacks but although the available resources within the network are limited additional techniques are needed beside cryptography to ensure the system security [10].

Several Approaches including steganography, physical layer secure access, data aggregation schemes, multilayer approaches and trust building are used integrally to provide a comprehensive defense line for the WSN. While cryptography aims to hide the content of transmitted packets steganography mechanism is capable of hiding the existence of the transmitted packets entirely, confusing the adversary who expects to get readings transmitted through the network [7]. Physical layer secure access strengthens the system security through frequency hopping in WSN, mainly by transmitting signals and quickly switching a carrier between several frequency channels. The effectiveness of this technique is lies in the efficient design for hopping order which is modified in less time compared to required time for discovery [9].

Multilayer defense approaches aims to guarantee WSN security in layers of protocols stack, providing a strong combination of malicious behavior prevention by employing a set of mechanisms at various layers within the OSI protocol. The main drawback of such approach is that the attack could be detected by several mechanisms causing in redundant detection and high power consumption [10].

Modeling trust in WSN is widely used for the early detection of malicious nodes and its subsequent effect prevention. Sensor nodes need to ensure the trust of the next node within the routing path to forward data packets, also the node needs to trust other neighbors to check anomalous readings. Several schemes had been proposed for trust modeling in WSN.

A. Trust management for resilient geographic routing (TM-RGR)

An algorithm is used to prevent attacks on geographic routing of data. The idea here is to reward a good behaving node and giving it additional confidence and trust raise every time it forwards a data packet successfully while punishing illegal node that lie about its location. Honest node remains longer time in the set of packet forwarding. After establishing a routing table for a specific node; it monitors the behavior of its next neighbor using snooping technique. TM-RGR is very simple and updating trust value does not take a lot of time, but in the other hand the accuracy is modest and the opportunity of false positives and false negatives is raised [13].

B. Hybrid Trust and Reputation Management (HTRM)

This scheme combines both behavior based approaches and certificate based approaches to update a node trust, behavioral based approaches depends on both direct and indirect behavioral information collected by the surrounding nodes. Trust of a node is calculated after gathering enough number of evidences from a certificate authority or any other trusted neighbor; in case where negative evidences are obtained the certificate is revoked immediately. As a result of the combination between certificates, direct and indirect behavior more power consumption is required for evaluating node trust which is not available within a single node [12].

C. Group Based Trust Management Scheme (GBTMS)

In this model instead evaluating the trust for a single sensor node, a light weight algorithm is used to evaluate the trust for a group of nodes within the WSN. A cluster head is capable of evaluating trust for sensor nodes within its cluster, and other cluster heads depending on both direct and indirect behaviors.

Memory consumption in GBTMS is minimized since trust of a group of nodes is evaluated and information is stored at the cluster head, but the amount of resources needed are more since the trust is calculated based on the previous behaviors [13].

D. Weighted Trust Algorithm (WTA)

WTA is used to detect the malicious nodes by observing its reported data to associate a weight for each node in the network. All sensing node are initialized with the same weight value. The a node weight is updated every cycle if it sends a report that differs from the reports of other sensing nodes. If a sensor node sends its report inconsistent with the final decision which is based on the reported data from others nodes its weight would be decreased and if it became lower than a specific threshold, the corresponding node will be identified as a malicious one. Weights are updated dynamically, but there is a high opportunity for false positive and false negative probabilities [14].

E. Behavior Trust based on Geometric Mean Approach (BTGMA)

BTGMA is a distributed trust scheme in which trust management is spread over the whole WSN; every node within the network is responsible for evaluating its trust based on direct and indirect behavior. Direct behavior is obtained by calculating the geometric mean of the quality of service (QoS) characteristics for a specific node, such as amount of consumed power, transmitted data rate, and reliability. Larger number of QoS characteristics employed larger the amount of consumed energy, and this is not consistent with the WSN limitations [13] [18].

F. Lightweight and Dependable Trust management Scheme (LDTS)

A light weight scheme is used for trust management in clustered WSN. Evaluating trust for a node is calculated depending on indirect evidences where indirect behavior is obtained using the feedback reported by cluster head node. LDTS improves system efficiency because it works even in cases where direct behavior is not accessible or insufficient, but the main drawback is its complete dependency on the cluster head, any unexpected damage in the CH disrupts the whole approach [8] [13].

G. Swarm intelligence based method.

Swarm intelligence approach is used to find the most reputable path in the network; nodes within this path are considered as trustworthy nodes and in result obtain a higher trust evaluation. Ant colony is a good example for swarm intelligence, searcher ants leave a pheromone in the path of food resource, where higher concentration of the pheromone higher attraction for collector ants to that path. Finding the shortest path between the source and destination node is computed easily using an algorithm such as Dijkstra's algorithm [8].

H. Artificial neural network method.

Neural networks have the ability to mimic the human brain behavior using a set of crude and simple approximations of the human neurons which is used to learn and generalize from training data. ANN consists of two main phases; training stage and generalization. In training phase weights of the input patterns are learned until a specific error is reached or after a specific number of iterations, so that the network learn the decision boundaries from the training patterns. Generalization phase includes using untrained inputs to find the output using the trained ANN, i.e. this phase is essential to classify untrained data correctly. ANN has many features that encourage its usage in WSN such as its parallelism, efficiency and noise tolerance which is very important in such harsh environment [15].

The existing ANN trust models based on calculating the trust rate of each node depending on its direct and indirect behavior which is obtained from the current and previous readings of its neighbors either in a cluster based network or any other topological WSN. The obtained reading which is called the expected reading is then compared with the actual one and trust rate is updated according to the convergence between both. The main drawback in the state-of-the-art ANN based trust models is the method for calculating node behavior. Nodes readings are treated equally without concerning about the spatial and temporal dimensions of these readings [16].

III. System Architecture

Providing a comprehensive WSN architecture that satisfies the robustness, availability and reduced power consumption is a challenging role. The current WSN architectures try to guarantee rationalized data delivery using star topology which reduces the consumed power by reducing the nodes within the transmission route. Several routing techniques are employed to minimize the wasted power by controlling the route for the transmitted data from sensing node to sink node. Concentrating on rationalizing the data transmission power consumption indicates that it consumes the largest portion of the available resources [17].

A. WSN components

WSN for water pollution monitoring system consists of several nodes equipped with sensors to get the concentration of water components in the surrounding environment, these nodes are collaborating together and linked via a wireless data link to the main node (sink node) that aggregates the collected readings from individuals, preprocesses and sends it to a main station to be processed and stored as shown in fig.1

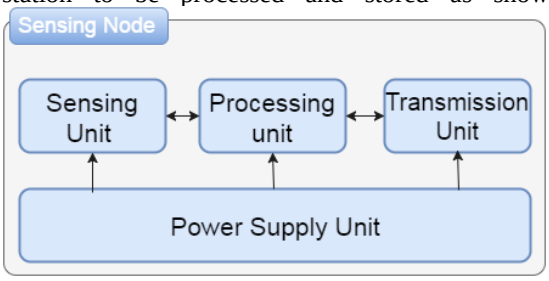

Fig. 1. WSN node components

microprocessor is the brain in each node, it is responsible for the basic processing of collected data via the sensing units, controlling the work of other node's components and managing the overall power consumption since each node has a

limited power resource, the main power consumption refers to the transmission of data which is the transceiver responsibility [17].

Water as a vital resource of life is polluted due to either chemical or natural changes. Natural water pollution includes the alteration of water natural properties due to increased salinity and temperature variation; so we need a sensor to measure water temperature and salt concentration. In the other hand chemical pollution implies water exposure to dangerous chemicals such as petroleum, arsenic and insecticides, these components change the properties of water and can affect the water potability. Sensing unit contains sensors to detect dangerous chemicals alongside with sensors that sense natural water pollution resources.

B. *Networking topology*

In WSN we proposed a cluster based WSN architecture that uses a hybrid network topology which combines star, mesh and ring topologies together. The three topologies are used to enhance the reliability of the system while taking in to account the available resources as following:

- a collection of the sensing nodes are connected to a central node cluster head(CH) that has an additional capabilities and resources among other nodes using star topology, as a result a set of clusters are obtained. Star topology has many advantages compares with other topologies including its scalability and power usage reduction; if a cluster head fail other nodes within the same cluster can reconfigure the topology and elect a new CH.
- Clusters heads are connected together as a mesh to provide a reliable communications, clusters heads had additional resources that facilitate the use of such topology. To access a specific cluster head the sink node needs an algorithm to detect the shortest path to that head to reduce consumed power as much as possible. All clusters heads are connected directly to the sink node which acts as a gateway to the outside world.
- Data collected through sensors in each node could be aggregated and sent to the base station by passing through the cluster head and sink node, if a node fail then the network will reconfigure itself around the other nodes, even if the radio link from a sensing node to its cluster head gone down due to interference for example then the access to that head would be done through an alternative ring connection, the ring path is chosen depending on the shortest path from the cluster head passing by the sensing node and returning to the head again. Fig.2 clarifies the overall architecture of WSN using hybrid network topology.

Cluster head aggregates the corresponding sensing nodes readings to be delivered to the base station via the sink node. Data delivery model decides when the collected data should be sent to the sink node, there are four main models for data delivery: continuous delivery, query driven, event driven and hybrid delivery models. Continuous delivery model sends the data periodically to the sink node while query driven models depend on the sink query for the data, event driven model depends on sending data when an event occurs. The proposed WSN system uses a hybrid data delivery model that enhances effective monitoring and enables the responsible party to take decisions accurately.

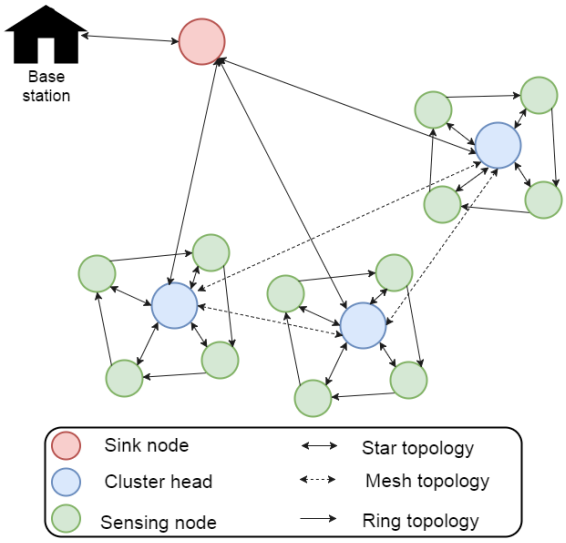

Fig. 2. System architecture

IV. Security in Wireless Sensor Network

Building Underground Water pollution monitoring system is a challenging task since several environmental conditions and changes may affect the WSN and cause in suspicious measurements as a result. For example a node could be disrupted due to environmental conditions or battery leakage, and that affects the availability of the system which is one of the main security goals for the WSN. A malicious node may enter the network and provide wrong data, change data or even transmit data about the validity and quality of the monitored water supply to another party; and this threatens the confidentiality and integrity of our system.

Generally, as any wireless sensor network built in a harsh environment the proposed system is exposed to security attacks such as DOS, wormhole, Sybil attack, hello flood and node-capturing attacks. The use of cryptographic algorithms alone cannot encounter and cope with the various types of attacks, so building trust between several nodes within the network is important to distinguish legitimate nodes from malicious ones [6].

V. Behavior Prediction in WSN using RBANN

Due to scalability, expandability and openness features of the WSN as a distributed system, additional new nodes can enter the system at different times; this exposes the network to several types of attacks and requires a strategy to distinguish legitimate nodes from foreign ones. Building trust is essential to assure the legitimacy of several nodes and protect the system so that no harmful node can masquerade or pretend to be a good one [9].

Different trust models have been proposed to provide an ultimate mechanism for detecting malicious nodes within WSN. All of the proposed trust models based on calculating

trust rate for every node within the system depending on its behavior which is captured by either direct or indirect fashion, depending on these rates the controller or director decide to consider a node as legitimate node and in result raise its trust rate or it could be a layer and punished by reducing its trust rate, if the rate decreased below a specific threshold the node may be discarded or monitored to be treated later [6].

ANN is widely used in real world approaches that build efficient systems to solve real world problems such as time series prediction. Employing ANN in Time series prediction applications is done by transferring the problem into a simple function that maps inputs to output using activations [16]. As shown in fig.3 predicting the reading of a sensor within the WSN is done depending on the previous n readings of the sensor as an input to the neural network, to accomplish the prediction based on both direct and indirect behaviors the network is expanded to include additional neighbors readings history.

Radial Base Artificial Neural Network uses three layers feed forward neural network; input layer, output layer and one hidden layer [19]. To predict the behavior of a node within the network the network works as following:

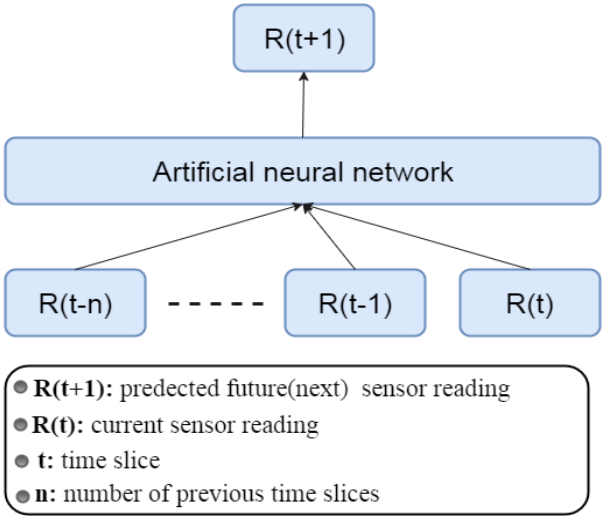

Fig. 3. Time Series Prediction using artificial neural network

- Input layer contains a set of readings (patterns) as input for nodes used in the direct behavioral prediction, but for indirect behavioral prediction the previous readings of other surrounding nodes are considered as a part of the input patterns.
- Single hidden layer that contains a set of radial bases functions (Gaussian functions) as an activation function to train the network from the available labeled readings. The training of ANN is essential to enable its ability to predict future readings of unlabeled patterns, the process can be described as preparing the network to be equipped for data it didn't see before and provide right predictions.
- Output layer implements a linear weighted sum function that calculates the predicted reading for a specific node.

Fig.4 shows how a RBFNN is used to predict the future reading of a sensing node based on its direct and indirect behavior. To find the activation function Φ(x) equation 1 is used [15]. The input to hidden basis function parameters $\{\mu, \sigma\}$ can be set using any number of unsupervised learning techniques.

$$\phi_j(\mathbf{x}) = \exp\left(-\frac{\|\mathbf{x}-\boldsymbol{\mu}_j\|^2}{2\sigma_j^2}\right) \quad (1)$$

Where j is a hidden neuron.

The output at output layer is calculated using both Φ(x) and weights from hidden to output layer as in equation 2.

$$y_k(\mathbf{x}) = \sum_{j=0}^{M} w_{kj}\phi_j(\mathbf{x}) \quad (2)$$

Where x- is the input value, j- is the hidden neuron; k is the output neuron, W_{kj} the weight from neuron k in hidden layer to neuron j in output layer.

Weights are trained and updated so that the sum-square output error is minimized; when the error is minimized to a specific threshold training is stopped and the network becomes ready for the generalization phase which is essential to assure the ability of the network to generalize from trained data and predict a correct reading for untrained samples, as a result the RBANN is capable of providing an expected reading for every node in the WSN for water pollution monitoring system. [15].

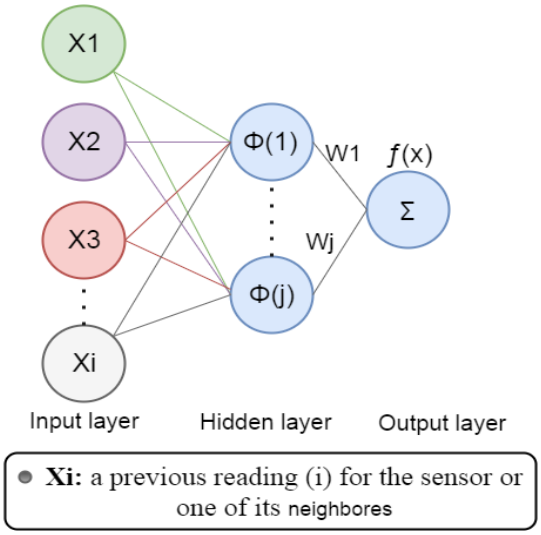

Fig. 4. Radial base neural network

VI. Proposed Trust Model

The proposed approach is to enhance the use of neural network for malicious nodes detection in WSN taking in to account the power supply and computational restrictions in such systems. A RBANN is used to find the expected reading of a node using a set of direct and indirect behaviors , the output is compared with the real reading of that node and the trust rate is then determined according to the convergence or divergence between both readings. Two main sequential stages are included in the proposed trust model:

A. Clusters heads trust rating.

To assure that a cluster head is not a malicious node and prevent it from distorting and changing sensed readings captured by sensing nodes within the same cluster, RBANN is used to calculate the expected behavior for that cluster head. Inputs of the ANN training are the n previous readings of the intended cluster head, current reading and previous n readings of other surrounding cluster heads, other clusters heads are given weight that determine the ratio with which each one affect the intended cluster head depending on the distance between both; shorter the distance larger the contribution in determining the expected behavior.

B. Sensing nodes trust rating.

RBANN is used to calculate the expected output and reading of each sensing node within each cluster using the previous and current readings of the remaining sensing nodes in the same cluster in addition to the previous n readings of the intended node. Each sensing node within the cluster affect the intended one with a specific ratio depending on the distance between both, also previous n readings for a node varies in its contribution based on the temporal differences between them, older the reading less its contribution in calculating a specific node expected reading.

Cluster heads passes the actual readings of all nodes to base station through the sink node. ANN resides in the base station where we have unlimited power and computational capabilities, that helps to avoid resources limitations in WSN. The expected readings obtained from the ANN is compared with the actual ones in database, if both are convergent trust rate is raised, otherwise trust rate is minimized. Generally trust rating for each sensing node is maintained according to the comparison between both actual and expected behavior.

As shown in fig.5 the proposed algorithm is constituted by the following steps which are applied periodically every time a sink node asks for sensed data:

1) Basically when the WSN system is constructed all nodes are initialized with equally trust rate such as 1.

2) The expected trust rate of each cluster head CHi is calculated based on the previous n readings of that head, current reading and previous n readings of all other cluster heads selected depending on the distance between each one of them and the CHi. Each cluster head affects the trust rate of CHi with R ratio depending on the distance between both and even previous n readings of a specific head have different proportions in calculating the cluster head expected reading depending on its time, older reading has less effect.

3) RBANN is calculates the expected output, if it converges to the current actual reading for that head then it is considered as trusted head and trust is raised; otherwise trust is minimized with respect to the variance between actual and expected reading as shown in fig.6.

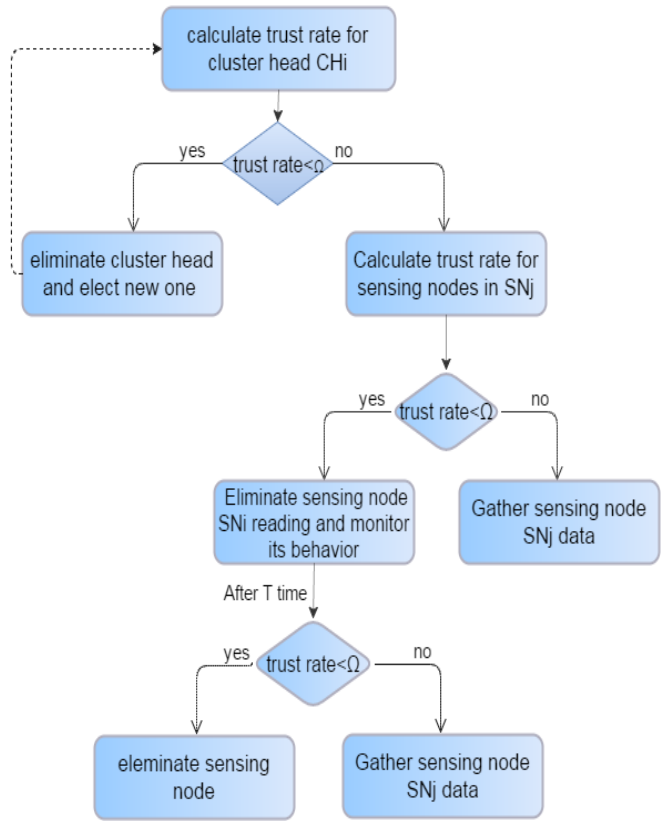

Fig. 5. Proposed algorithm for trust rate calculation

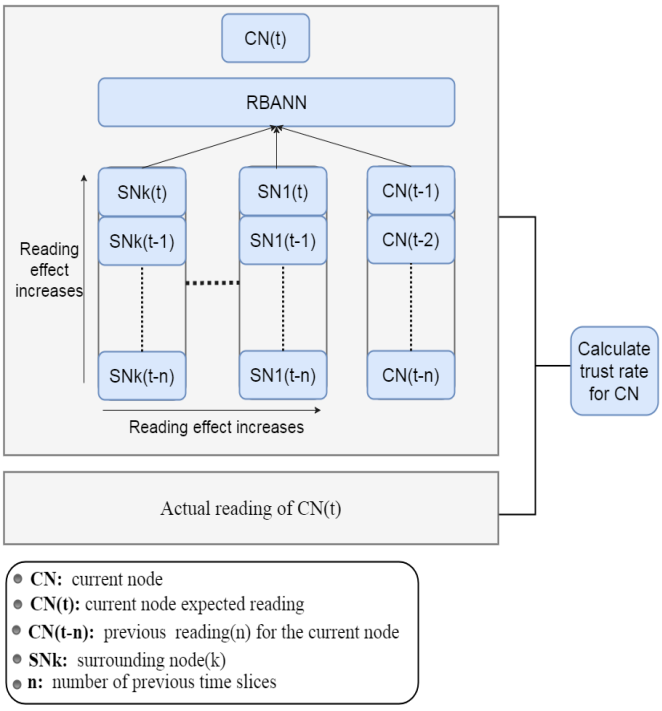

Fig. 6. WSN node trust rate calculation

4) If trust rate for a specific cluster head became less than a specific threshold Ω cluster head is eliminated and another new one from the same cluster is elected, the winner is the richer node which has abundant available resources compared to other cluster nodes.

5) After ensuring the trust of a cluster head, corresponding sensing nodes trust within the same cluster need to be checked. As in fig.6 trust rating for each sensing node is done by comparing its actual reading passed to the base station by a trusted cluster head and the corresponding expected one obtained using the ANN. The inputs to ANN are the n previous readings of the intended node, current and n previous readings for all sensing nodes within the same cluster. Each sensing node contributes in calculating the expected trust rate depending on its distance from the intended one, closer the distance larger the influence in calculations.

6) If the trust rate is raised, sensing node is considered a trusted one and its gathered data is considered as a valuable data, otherwise trust rate degrades and after it becomes smaller than Ω the node is considered a suspicious one and its reading is discarded for t of time while its behavior under monitoring, if the node behavior didn't improve then it is considered a malicious one and its collected data discarded, otherwise trust rating improves and became more than Ω so the node is reconsidered trustful and its readings are taken in to account.

Since cluster head has larger influence, permissions and effect on the system as a whole in more comprehensive fashion, a suspicious cluster head will be eliminated directly without any other considerations because it is capable of influencing and harming the entire system by either changing the collected data sent from sensing nodes within the same cluster or even by providing a misleading trust rate evaluation of other cluster heads.

Employing the proposed algorithm provides the administrator at the base station with a mean to track the trust of all network nodes and eliminate malicious or damaged ones. The implementation of the algorithm in two sequential hierarchical stages helps to reduce the consumed power for strangers' detection and also reduces the wasted efforts in case where a cluster head masquerades or forges nodes within the same cluster, exactly as any hierarchal arrangement the higher branch always affects all other sub-branches so credibility of a cluster head is checked to trust what it passes to the base station.

VII. CONCLUSION

WSN used for Water pollution monitoring system requires a powerful defense line against threats and changes in the surrounding, taking in to account resources challenges in such system. Enhanced ANN based trust model is proposed to overcome the weaknesses in the existing WSN trust models. By using a modified radial base ANN we improve the way in which ANN is used to predict the expected readings of network nodes, and calculate their trust rate based on spatial and temporal weighting of both sensing nodes, and clusters heads. In addition we adapted a dependable, fault tolerant hybrid architecture that combines mesh, star and ring topologies in order to provide a comprehensive robust WSN that consumes less resources compared with the existing WSN. In the future work we aim to improve RBANN accuracy using additional inputs to represent the direct behavior for the node being evaluated depending on the geometric mean of its quality of service (QoS) characteristics.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, December 2011.

[2] N. Rodriguez, S. Rossetto, "Distributed systems with wireless sensor networks," 2012.

[3] Q. Mamun, "A qualitative comparison of different topologies for wireless sensor networks," 2012.

[4] A. Devasena, B. Sowmya, "Wireless sensor network in disaster management," Indian journal of science and technology, July 2015.

[5] A. K. Pathan, H. W. Lee, C. S. Hong, "Security in wireless sensor networks: Issues and challenges," ICACT, 2006.

[6] M. Momani, S. Challa, "Survey of trust models in different network domains," 2010.

[7] W. Stallings, "Cryptography and Network Security," sixth edition, 2013.

[8] V. U. Rani, K. S. Sundaram, "Review of Trust Models in Wireless Sensor Networks," International scholarly and scientific research & innovation, 2014.

[9] H. Rathore, H. Badarla, S. Jha, A. Gupta, "Novel approach for security in wireless sensor network using bio-inspirations," IEEE, 2014.

[10] G. Kulkarni1, R. Shelk , K. Gaikwad, V. Solanke , S. Gujar , P. Khatawkar, "Wireless sensor network security threats," IET, July 2015.

[11] E. P. k Gilbert, B. Kaliaperumal, and E. B. Rajsingh, "Research issues in wireless sensor network applications: A survey," International journal of information and electronics engineering, September 2012.

[12] H. A. N Jitender, S. Deogun and E. D. Manly, "Secure and energy aware routing against wormholes and sinkholes in wireless sensor network", IEEE, 2006.

[13] R. W. Anwar, M. Bakhtiari, A. Zainal and K. Naseer Qureshi, "A survey of wireless sensor networks and routing techniques," Research Journal of Applied Sciences, Engineering and Technology, 2015.

[14] V. Reshmi, M. Sajitha, "A Survey on trust management in wireless sensor networks," International journal of computer science & engineering technology, February 2014.

[15] S. Haykin, "Neural networks and learning machines," third edition, 2009.

[16] A. Doboli, "Discovery of malicious nodes in wireless sensor networks using neural predictors," WSEAS transactions on computer research, February 2007.

[17] S. Sharma, D. Kumar and K. Kishore, "Wireless sensor networks- A review on topologies and node architecture," International journal of computer sciences and engineering open access, 2013.

[18] 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, JUNE 2012.

[19] M. Awad, H. Pomares, I. Rojas1, O. Salameh and M. Hamdon, "Prediction of time series using RBF neural networks: A new approach of clustering," The International Arab Journal of Information Technology, April 2009.

AUTHOR PROFILE

Adwan Yasin is an associate Professor, Former dean of Faculty of Engineering and Information Technology of the Arab American University of Jenin, Palestine. Previously he worked at Philadelphia and Zarka Private University, Jordan. He received his PhD degree from the National Technical University of Ukraine in 1996. His research interests include Computer Networks, Computer Architecture, Cryptography and Networks Security.

Kefaya Saba'neh is a Computer Science master student in the Arab American University of Jenin, she also received her bachelor degree in Multimedia Technology from the Arab American University of Jenin in 2010.