International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 3 (September '2017)
Proceeding of - International Conference on Recent Trends in Computational Life Science and Information Technology,
Conference held at Tiruppur Kumaran College for Women,Tirupur,Tamilnadu, India.

ACTIVE TRUST: SECURE AND TRUSTABLE ROUTING IN WIRELESS SENSOR NETWORKS

M.Kavitha,
Assistant Professor,
Department of Computer Science,
Tiruppur Kumaran College for Women,
Tiruppur, Tamilandu, India.

K.Hemapriya,
Research Scholar,
Department of Computer Science,
Tiruppur Kumaran College for Women,
Tiruppur,Tamilandu, India.

Abstract: Wireless sensor networks (WSNs) are increasingly being disposed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. To conquer that challenge in the existing system, an active detection-based security and trust routing scheme named ActiveTrust is introduced for WSNs. ActiveTrust can extremely increase the data route success probability and across against black hole attacks and can optimize network lifetime. However in the existing system, the computation overhead is high which finding the trustable detection routes in case of presence of higher nodal density where the request needs to be traversed through all nodes, The existing work only concentrates on detection of black hole attacks which doesn't consider the grey hole attacks present in the network. This is resolved in the proposed system by concentrating secured and trustable routing which can improve the overall performance of the wireless sensor network with improved packet delivery ratio. This is done by filtering out the packets with less trust value to avoid the unwanted transmission of control packets. This is done by introducing the new method namely Trust based Packet Filtering (TPF) where the packets with less trust values would not be considered for the further packet transmission. In addition to that Trust and Density aware Clustering (TDC) method is introduced to avoid the more computation overhead. And also in this research work, security is enhanced by finding the grey hole attacks along with black hole attacks. Here adversary nodes are identified based on the information gathered from the neighbor nodes by using which more optimal cluster head is selected. Thus the optimal and secured routing can be ensured in the wireless sensor network which would increase the WSN contribution.

Keywords: grey hole attack; black hole attack; trust based filtering; densityawareclustering; sensor network.

I.INTRODUCTION

Wireless communication is the transfer of information or power between two or more points that are not connected by an electrical conductor. The most common wireless technologies use radio. With radio waves distances can be short, such as a few meters for television or as far as thousands or even millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular, personal digital assistants (PDAs), and wireless networking. Other examples of applications of radio wireless technology include GPS units, garage door openers,
wireless computermice, keyboards and headsets, headphone s, radioreceivers, satellitetelevision, broadcasttelevision and cordless telephones [1]. Recent advances in wireless communications and electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks. Sensor networks represent a significant improvement over traditional sensors [2]. To prolong the networks lifetime, minimization of energy consumption should be implemented at all layers of the network protocol stack starting from the physical to the application layer including cross-layer optimization. Optimizing energy consumption is the main concern for designing and planning the operation of the WSN. Clustering technique is one of the methods utilized to extend lifetime of the network by applying data aggregation and balancing energy consumption among sensor nodes of the network. In clustered networks, Sensor nodes in each cluster transmit their data to the respective Cluster Head (CH) and the CH aggregates data and forwards them to a central base station [3]. More energy is drained from Cluster Heads (CHs) due to message transmission over long distances (CHs to the base Station) compared to other sensor nodes in the cluster [4]. It is essential to avoid quick depletion of cluster heads.The optimal election and re-election of CHs, and cluster maintenance are the main issues to be addressed in designing of clustering algorithms. Hence this thesis proposes methods for selection of cluster head based on meta-heuristic algorithms like Firefly Algorithms (FA), Artificial Bee Colony Algorithms (ABC), Particle Swarm Optimization (PSO) and Shuffled frog leap algorithms (SFLA) for increasing the lifetime of the WSN. The

following sections will discuss the architecture of WSN and related issues and challenges in it [5].

II. RELATEDWORKS

A detection route indicate to a route without data packets whose goal is to satisfy the adversary to launch an attack so the system can find the attack behavior and then tick the black hole location. Thus, the system can lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Via active detection routing, nodal trust can be quickly secured, and it can exclusively guide the data route in choosing nodes with high trust to avoid black holes. In this scheme, the source node randomly selects an undetected neighbor node to create an active detection route. Assuming that the longest detection route length is w, the detection route minimizes its length by 1 for every hop until the length is decreased to 0, and then the detection route ends. The data routing refers to the process of nodal data routing to the sink. The routing protocol is similar to common routing protocols in WSNs; the difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink. The routing protocol can adopt an existing routing protocol, and we take the shortest route protocol as an example. Node a in the route will choose the neighbor that is nearer the sink and has high trust as the next hop. If there is not a node among all neighbors nearer the sink that has trust above the default threshold, it will report to the upper node that there is no path from a to the sink.The upper node, working in the same manner, will re-select a different node from among its neighbors nearer the sink until the data are routed to the sink or there is conclusively no path to the sink. The content of the detection routing packet can be divided into 6 parts: (a) packet head; (b) packet type; (c) ID of the source node; (d)
maximum detection route length; (e) acknowledge returned to the source for every ωhops; and (f) ID of the packet. The source node selects an undetected node to launch the detection route. Once the detection packet is received by nodes, the maximum route length ωis decreased by 1. After that, if ωis 0, generate a feedback packet and launch a feedback route to the source, and then restore ωto the initial value. If ωis not 0, then continue to select the next hop in the same way; otherwise, end the route.The feedback packet is routed back to the data source; because nodes cache the detection route info, the feedback packet is able to return back to the source, and the algorithm for the detection route protocol.

III. THE SYSTEM MODEL

(a) We consider a wireless sensor network consisting of sensor nodes that are uniformly and randomly scattered in a circular network; the network radius is R, with nodal density ρ, and nodes do not move after being deployed. Upon detection of an event, a sensor node will generate messages, and those messages must be sent to the sink node.(b) We consider that link-level security has been established through a common cryptography-based protocol. Thus, we consider a link key to be safe unless the adversary physically compromises either side of the link.we consider that black holes are formed by the compromised nodes and will unselectively discard all packets passed by to prevent data from being sent to the sink. The adversary has the ability to compromise some of the nodes. However, we consider the adversary to be unable to compromise the sink and its neighboring nodes.

3.1. ACTIVE TRUST MODEL

A detection route refers to a route without data packets whose goal is to convince the adversary to launch an attack so the system can identify the attack behavior and then mark the black hole location. Thus, the system can lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Through active detection routing, nodal trust can be quickly obtained, and it can effectively guide the data route in choosing nodes with high trust to avoid black holes. In this scheme, the source node randomly selects an undetected neighbor node to create an active detection route. Considering that the longest detection route length is w, the detection route decreases its length by 1 for every hop until the length is decreased to 0, and then the detection route ends. The data routing refers to the process of nodal data routing to the sink. The routing protocol is similar to common routing protocols in WSNs; the difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink. The routing protocol can adopt an existing routing protocol, and we take the shortest route protocol as an example. Node a in the route will choose the neighbor that is nearer the sink and has high trust as the next hop. If there is not a node among all neighbors nearer the sink that has trust above the default threshold, it will report to the upper node that there is no path from a to the sink. The upper node, working in the same manner, will re-select a different node from among its neighbors nearer the sink until the data are routed to the sink or there is conclusively no path to the sink.

3.2. ACTIVE DETECTION ROUTING PROTOCOL

The content of the detection routing packet can be divided into 6 parts: (a) packet head; (b) packet type; (c) ID of the source node; (d) maximum detection route length; (e) acknowledge returned to the source for every ωhops; and (f) ID of the packet. The source node selects an undetected node to launch the detection route. Once the detection packet is received by nodes, the maximum route length ωis decreased by 1. After that, if ωis 0, generate a feedback packet and launch a feedback route to the source, and then restore ωto the initial value. If ωis not 0, then continue to select the next hop in the same way; otherwise, end the route.

The feedback packet is routed back to the data source; because nodes cache the detection route info, the feedback packet is able to return back to the source, and the algorithm for the detection route protocol

IV.PROPOSED METHODOLOGY

In the existing system, the computation overhead is high which finding the trustable detection routes in case of presence of higher nodal density where the request needs to be traversed through all nodes, The existing work only concentrates on detection of black hole attacks which

doesn't consider the grey hole attacks present in the network. This is resolved in the proposed system by concentrating secured and trustable routing which can improve the overall performance of the wireless sensor network with improved packet delivery ratio. The different methods have been proposed in this research work to ensure the guaranteed level of security and trust of users. In the proposed research work, computation overhead is reduced by decreasing the number of control packets sent over the undetected nodes for finding the detection route. This is done by filtering out the packets with less trust value to avoid the unwanted transmission of control packets. This is done by introducing the new method namely Trust based Packet Filtering (TPF) where the packets with less trust values would not be considered for the further packet transmission. In addition to that Trust and Density aware Clustering (TDC) method is introduced to avoid the more computation overhead. And also in this research work, security is enhanced by finding the grey hole attacks along with black hole attacks. Here adversary nodes are identified based on the information gathered from the neighbor nodes by using which more optimal cluster head is selected. Thus the optimal and secured routing can be ensured in the wireless sensor network which would increase the WSN contribution.

4.1. TRUST BASED PACKET FILTERING

In this work, we develop two types of trust values: node trust and overall IP confidence. Node trust is used to evaluate the trustworthiness of a node, while overall IP confidence is used to evaluate the trustworthiness of an IP address, which can help generate a blacklist accordingly.

Node trust. In a collaborative environment, this kind of trust value aims to evaluate the trustworthiness of a node. According to the basic CIDN framework, the trustworthiness of a node can be calculated based on its responses to challenges. The challenges are sent out periodically by means of a random process. After receiving an answer to a challenge, a satisfaction level can be computed through identifying the gab between the received feedback and the expected answer. It is worth noting that the feedback from a node is ordered from the most recent to the oldest according to tk. As a result, the trust value of node i according to node j can be computed as below:

$$T_{node}^{i,j\,\prime} = w_s \frac{\sum_{k=0}^{n} F_k^j \lambda^{tk}}{\sum_{k=0}^{n} \lambda^{tk}}$$

Where $F_k^j \in [0,1]$ is the score in relation to the received feedback k, n is the total number of feedback, $\lambda \in [0; 1]$ is a forgetting factor that assigns less weight to older feedback response, ws is a significant weight depending on the total number of received feedback, m is the number limit of received feedback. If the number of feedback is smaller than m, then $w_s = \frac{\sum_{k=0}^{n} \lambda^{tk}}{m}$; otherwise $w_s = 1$. Note that m aims to encourage those nodes with high request frequency to send back answers, and its value can be adjusted based on the high request frequency of challenges.Additionally, based on the CIDN design from [10], [11], 'unsure' answers are acceptable from an IDS node, when this node has no information about the challenges. This mechanism is especially beneficial for a newly joined IDS node that has no experience for the environment. However, a malicious node may use this mechanism to maintain its trustworthiness, there is a need to punish a node if it sends too many 'unsure' answers. Thus, the trustworthiness of node i according to node j can be further calculated as below

$$T_{node}^{i,j} = \left(T_{node}^{i,j\,\prime} - T_{initial}\right)(1-x)^y + T_{initial}$$

where $x \in [0; 1]$ is the percentage of 'unsure' answers from time t_0 to t_k, y is a positive parameter to control the severity of punishment on such answer, which can be computed based on the received feedback. Tinital is the default trust value of a new node. According to the above equation, a node's trust value would decrease, if it sends a large number of 'unsure' answers (namely a large x).

Overall IP confidence. As mentioned above, IP confidence is used to evaluate the trustworthiness of an IP source. In a collaborative network, trust computation can consider the data from other trusted IDS nodes in addition to the information from the node itself. To achieve this, we define a metric of overall IP confidence (Toic) to represent the overall trustworthiness of an IP source. In terms of this metric and a threshold, the packet filter can reduce unwanted packets accordingly. If a node j wants to evaluate a target IP, then $T_{oic}^j(IP)$ can be calculated as below:

$$T_{oic}^j(IP) = \frac{\sum_{T_{node}^{i,j} \geq r} T_{node}^{i,j} D_i^j T_{oic}^i(IP)}{\sum_{T_{node}^{i,j} \geq r} T_{node}^{i,j} D_i^j}$$

where r is a trust threshold, so that node j has to request the information (e.g., IP confidence) from those nodes whose trust values are higher than $r.T_{node}^{i,j}$ ($\in [0; 1]$) indicates the trust value of node i according to node j. $D_i^j (\in [0; 1])$ is a measure of geographical distance between node i and node j. $T_{oic}^i(IP) (\in [0; 1])$ describes the IP confidence of a target source, which is computed by node i.Based on these trust values filtering would be done in the proposed research methodologies where the node with less trust values would not be considered for the next routing. So that secured data communication can be ensured.

4.2. TRUST AND DENSITY AWARE CLUSTERING

Inspired by Darwin's theory, GA starts with a set of solutions (represented by chromosomes) called a population. Solutions from one population are taken and used to form a new population. This is motivated by a hope that the new population will be better than the old one. Solutions which are selected to form new solutions (offsprings) are selected according to their fitness - the more suitable they are the more chances they have to reproduce. The fundamental fragments of a GA are explained below.

4.2.1. Crossover

In crossover, two parents are selected based upon the fitness. They are used to reproduce a new offspring. It is assumed that the offspring will inherit the good characteristics of both the parents and will have better characteristics than its parents. For example consider the below scenario where two parents are taking part in the one point crossover, where a random crossover point is selected and bits of the parents' chromosomes are swapped at that point to create a new

offspring [2,3,9]. The below example shows the results, before and after cross over.

4.2.2. **Mutation**

In mutation, a bit, which is 0 becomes 1 and the bit which is 1 becomes 0. Mutation is applied at mutation probability. After mutation, regular node may become a cluster head and a cluster head may become a regular node. When a CH becomes a regular node, members of that cluster join nearest CH and if a regular node becomes the CH, the nodes which are close to it join this cluster [4, 5].

4.2.3. **Selection**

Selection is used to select chromosomes for mating process i.e. crossover. Mating process reproduces new chromosomes, which join current population. This is thencalled as a new generation.

4.2.4. **Fitness function**

This is the function of various fitness parameters used to evaluate the fitness of the chromosomes. Fittest chromosomes are used to create a new population.The proposed system adapts GA parameters to determine the CH and then forms the cluster around it based on the shortest distance between CH and member sensor nodes. Two parameters are considered for the selection of CHs. The first parameter is where the fitness of all the nodes is calculated and then genetic operators such as crossover and mutation on the chromosomes are applied.The second parameter is based on the trust of that node, which is calculated by the number of successful and unsuccessful events that passed through it. Once both the parameters are fulfilled, the node with the highest energy and highest trust becomes the CH. Once the CHis selected, it clusters and then the sensed data are transferred from CH to CH to Sink through multihop routing protocol, which helps to reduce energy consumption and in turn increases the network lifetime.

V. EXPERIMENT CONFIGURATION AND RESULTS

This section discusses the experiment and its results.

5.1 EXPERIMENT

The experimental results were conducted in NS2 simulator, were the performance of the proposed research methodologies are evaluated. The network topology of a100m X 100m of randomly distributed heterogeneous nodes with their initial energies varying between 0.5J to 2.25J is used and BS is positioned in the center of the network system. In order to be fair, the energy of the system on an overall for every protocol is assured to be the same; a total energy of 102.5J has been used. In addition, the optimal parameters of these protocols are used for yielding their corresponding best performance. To evaluate the performance of the proposed approaches, several parameters are used as such as Energy Consumption, Throughput, End-to-end delay (EED), Packet Delivery Ratio and Routing overhead.

5.2 PERFORMANCE EVALUATION

This work considered the following important Performance metrics for the evaluation by simulation. Here proposed research method namely Trust aware Routing in WSN (TR-WSN) is compared with the existing research methods LEACH, and ActiveTrust. Energy consumption is defined as the total energy consumed for completing the successful data transmission. Energy consumption of the proposed research method should be lesser than the existing research methods for the better performance. Energy consumption comparison values are shown

Number of nodes	Energy Consumption		
	LEACH	Active Trust	TR-WSN
20	100	92	89
40	140	132	130
60	170	163	168
80	200	182	188
100	250	232	238

Table 1: Energy consumption Vs No. of Nodes

Table: 1 illustrates the relationship between the Energy consumption on communications and the number of nodes. It can be said that the proposed TR_WSN approach consumes less energy when compared with the other proposed Activetrust the existing LEACH approach. This is due to the cluster head selection algorithm the cluster heads will be selected from the sensor nodes based on the calculation made using certain factors in every nodes. Based on the distance between the nodes, mobility of the nodes, residual energy and transmission range of the neighborhood nodes the weight of the each node will be calculated in efficient manner. The other algorithms are lack in calculating the residual energy between the nodes while transmitting the packets. The performance of Energy consumption by nodes is observed to be still lesser for further increasing nodes too.

VI. CONCLUSION

Preserving security and confidentiality in wireless sensor networks (WSN) is crucial. In WSN, a third person can eavesdrop to the information or link to the network. So, preventing these intrusions by detecting them has become one of the most demanding challenges. The clustered wireless sensor networks are incapable of satisfying resource efficiency and trust system because of the high overhead and low dependability. Many trust systems are used in WSN which employs the Clustering Algorithm. The existing trust system uses a self-adaptive feedback model for trust evaluation. Even though this enhances the energy efficiency and confirms the trustworthiness of nodes that participate in the communication, there are certain drawbacks. The trust values can be analyzed by an intruder and also there is no authentication for the messages being transmitted. The main characteristics of WSN's are their limited processing, storage, bandwidth and energy. To solve all of these problems, the proposed work is carried out in three ways. ActiveTrust can significantly improve the data route success probability and ability against black hole attacks and can optimize network lifetime.

VII. REFERENCES

[1]. Akyildiz, IF, Su, W, Sankarasubramaniam, Y &Cayirci, E 2002, 'A survey on sensor networks', Communications Magazine, IEEE, vol.40, pp.102-114.
[2]. Pottie, GJ & Kaiser, WJ 2000, 'Wireless integrated network sensors', Communications of the ACM, vol.43, no.5, pp.51-58.
[3]. Gupta, G &Younis, M 2003, 'Fault-tolerant clustering of wireless sensor networks', Proceedings of the IEEE Wireless Communication and Networks Conference (WCNC), New Orleans, Louisiana, pp.1579- 1584.
[4]. Bandyopadhyay, S & Coyle, E 2003, 'An energy efficient hierarchical clustering algorithm for wireless sensor networks', Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), San Francisco, California, vol.3, pp.1713-1723.
[5]. Michael, L, Raymer, William, F, Punch, Erik, D, Goodman, Leslie, A, Kuhn, & Anil, K, Jain 2000, 'Dimensionality Reduction Using Genetic Algorithms,' IEEE Trans. Evolutionary Computation, vol.4, no.2, pp.164-171.
[6]. Heinzelman, WR, Chandrakasan, A &Balakrishnan, H 2000, 'Energy-efficient communication protocol for wireless micro sensor networks', Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, pp.3005-3014.
[7]. Krishnamachari, B, Estrin, D & Wicker, S 2002, 'Modelling data centric routing in wireless sensor networks', Proceedings of IEEE INFOCOM, New York, NY, pp.1-11.
[8]. Murugunathan, SD, Ma, DCF, Bhasin, RI &Fapajuwo, AO 2005,'A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks', IEEE Radio Communication, vol.43, pp.8-13.
[9]. Vidhyapriya, R &Vanathi, PT 2007, 'Conserving energy in wireless sensor networks', IEEE Potentials, vol.26, pp.37-42.
[10]. Chang, JH &Tassiulas, L 2004, 'Maximum lifetime routing in wireless sensor networks', IEEE/ACM Transactions on networking, vol.12, no.4, pp.609-619.
[11]. SanatanMohanty 2010, 'Energy Efficient Routing Algorithms for Wireless Sensor Networks and Performance Evaluation of Quality of Service for IEEE 802.15.4 Networks', National Institute of Technology, Rourkela-769008, pp.1-127.
[12]. Y. Wang, G. Attebury and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks", IEEE Communications Surveys and Tutorials, vol. 8, pp. 2-23, 2006
[13]. Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location-based Compromise Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE Journal on Selected Areas in Communications, vol. 24, pp. 247-260, 2006.
[14]. Z. Liu, A. W. Joy and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks", in Distributed Computing Systems, 2004. FTDCS 2004., 2004
[15]. D. Zhou, "Security Issues in Ad-hoc Networks", in The Handbook of Ad-hoc Wireless Networks Boca Raton, FL, USA: CRC Press, Inc. , 2003, pp. 569 - 582.