Even Data Distribution Scheme To Avoid Attacks By Increasing Network Performance

N.Divya, Dr. R. Muralidharan

Abstract : Due to expansion of cyber-attacks, the network faces issues in tolerating the node failures, thus enhancing the WSN's robustness is the best way to improve the networks robustness. WSN with high performance and QoS are needed, because they overcome the random attacks, but they become unsafe to malicious attacks that especially focus on certain significant nodes. The performance of existing approaches in maintaining the network performance, however, degrades in large scale networks rapidly with lossy links. When the data packets are sent continuously through the high performance node, the attackers find it easy to just concentrate on those particular nodes for acquiring data. To avoid this, we introduce even data distribution scheme, where the data are forwarded evenly among the nodes by considering their hop count i.e., hop count should be minimum. Hybrid data distribution algorithm is implemented for even distribution among nodes, routing path is chosen by hop count of nodes. Then the data packets are forwarded by clustering by setting the limited threshold I^{thr}. The parameters obtained from simulation results that are carried in NS-2 are delay, overhead, and PDR. Our proposed scheme presents much better scheme, thus reducing the delay and overhead in network in turn increasing the PDR.

Index Terms: WSN, Distribution algorithm, Threshold, PDR, Delay, Hop count, Overhead.

1. INTRODUCTION

Wireless networks have self dependent nodes disseminated in space which are effectively deployable in unfavorable conditions for monitoring the ecological conditions, for example, temperature, pressure and noise. These nodes are equipped for data transfer from one node to another with no physical medium [1]. For transferring data, source node can straightforwardly associate with destination node or may interact with intermediate nodes which go about as an interface among source and destination nodes. Such system with intermediate nodes is known as multi-hop systems [2]. WSN gives an entrance which goes about as an interface between end client to process the transmitted data by the sensor nodes. Such kind of network represents a few constraints. As the nodes are broadly spread, WSNs are presented to different malicious attacks [3] because all the data packets are forwarded via high performing or high capacity nodes where else the other nodes becomes idle. This misguides the other nodes present in the network and causes overhead [4] in network. The other major problem is that, when data packets are sent continuously through the high capacity nodes is that the occurrence of malicious attacks by the attackers increases. The attackers or hackers find it easy to control just one high performing node than all nodes in network. And also there is delay and congestion in network when the data packets are sent via same nodes. The sender thinks that it is the easy method to reach destination but the existing system fails to address the congestion and delay that occurs when using the same node for data transmission. The energy is consumed by the idle nodes in a network which affects the performance of the network. To overcome all the drawbacks in network, the data's must be distributed evenly among the selected nodes. The proposed scheme, an upgraded, dependable, and secured even distribution of data scheme uses Hybrid data distribution algorithm where the data's are transmitted by selecting the routing path efficiently. The routing path is decided based on the nodes hop count [5]. The nodes with minimum hop count are chosen and the routing path is built. Once the nodes and routing path [6] is selected, the data packets are transmitted by forming clusters. Generally the clusters in WSN are formed to diminish the communication overhead in network and help to decrease the energy consumption. To achieve the even data distribution, the model network is been created initially and then the data packets are distributed evenly. Our proposed model avoids the unwanted exposure of the data to the attackers, provides higher security and the performance of the network is increased. Rest of this paper is arranged as, i.e., in Section II, a short survey of related work is presented. Section III describes our proposed methodology. Section IV introduces the basic ideas of our new even data distribution scheme and describes the parameters considered and the proposed algorithm is explained in this section. In section V, We show the simulation results and the outputs obtained. Finally, in Section VI we precise the conclusion and future work.

2. RELATED WORK

For distributed data storage in Wireless Sensor Networks, security issues have been focused on by extensive researches in recent years. The past work on this is analyzed to implement the proposed system. Y. Ren et al [7] proposed secure and reliable data distribution scheme. This scheme can give probabilistic backward secrecy, data reliability and forward secrecy. An optimized scheme for data distribution is proposed. Khan M.F [8] have presented and compared the performance of different network topologies for WSN that can be implemented in mission critical industrial applications. Two performance parameters, delay and PDR are analyzed in this study. W. Cheng et al [9] proposed a novel secure and repairable scheme for distributed storage of data in UWSNs. It takes advantage of both EC and SRC, to achieve better security on data storage and redundancy maintenance. W. Cheng et al [10] proposed a reliable, secure and enhanced scheme for distributing data using erasure codes for UWSNs which takes the MOVE-ONCE strategy for survival. Here the authors have utilized two-hop neighbor set as data shareholders for data distribution.

3. PROPOSED METHODOLOGY

The major problem faced in the WSN is threat of attacks due to frequent usage of high performing nodes in the network. In existing, there is no specific method or scheme to distribute the data evenly among nodes to rectify this, instead the existing work concentrated to rectify the malicious attacks after it occurs. In proposed we propose

even data distribution scheme by implementing Hybrid data distribution algorithm. The network model is formed by bringing the needed nodes to form the network. After that the packets must be transferred via routes. Routing [11] path is identified from source to forward data tp destination by analyzing the hop count in a choosing path. Once the routing process is over, data packets are forwarded by cluster formation with some threshold limit, I^{thr}. This threshold is relies on the bandwidth of transmitting data, carrier power C_p, carrier sense C_s and the radius R_x.

Architecture of proposed system

The flow of our proposed work is shown in architecture diagram in figure 1. Initially the network is built to initiate the data transmission to destination from source. The nodes for sending the data are chosen by considering carrier power C_p, carrier sense C_s and the radius R_x. The hop count is considered for routing, hop count is for finding the shortest distance from source to destination.

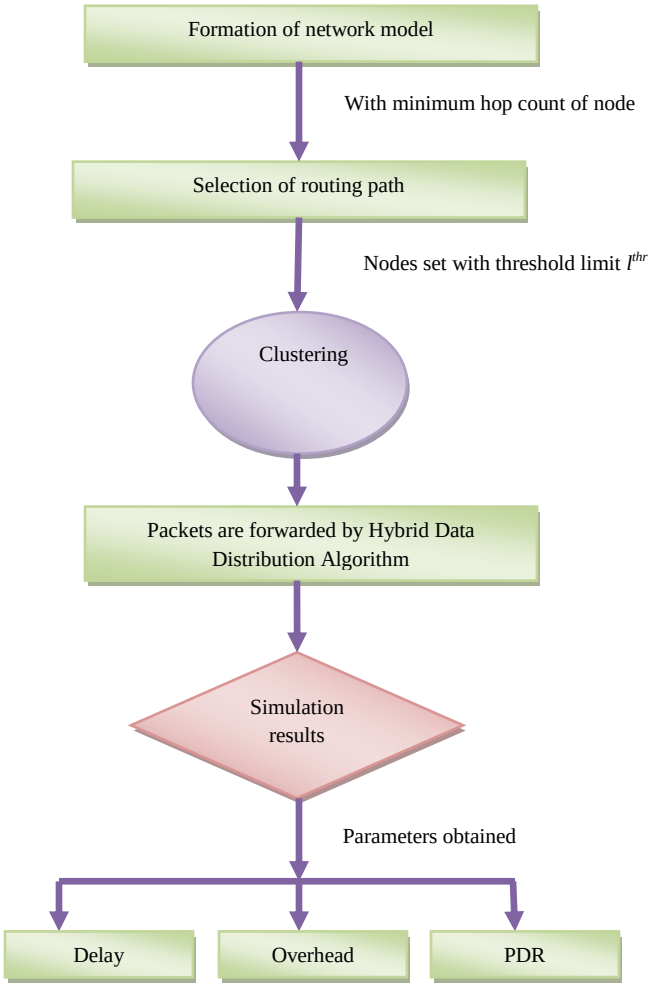

Figure 1. *Architecture of proposed system*

After the routing process is done, the data is formed as clusters to avoid the time delay and overhead. In WSN, the performance should be increased and the delay in the network must be reduced. The process of work model is explained briefly in the following sections.

Network Model

Our network consists of wireless sensor nodes distributed randomly in an untrusted environment. Every node has its own capacity and energy level. The other main parameter considered in our method is hop count of every node which helps to form the routing path. The nodes are selected accordingly with low hop count. To use all the selected nodes efficiently, our network is built where in existing only the high performing nodes were utilized for data transferring. The network is formed with ring topology with MAC protocol [12] in the application layer. MAC protocol is scalable and adaptable, i.e., they can adapt themselves in continuously changing environment such as density of node, topology or size of nodes. Figure 2 illustrate the formation of network model and the placement of nodes in the network. And also among all nodes, the 6th node is set as source and 4th is set as destination nodes are also being set.

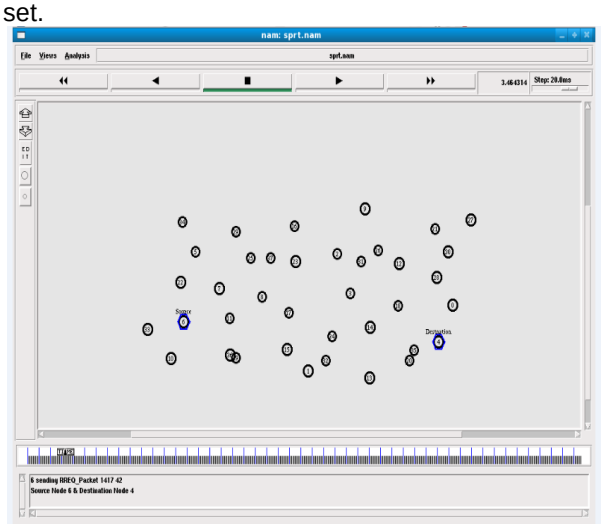

Figure 2. *Proposed Network Model*

Every node forward packets to neighboring nodes those are in its range. The transmitted power p confines the range for communication. Every node receives the packet from its adjacent nodes and every node is accountable for transferring the data to destination. The main objective is to forward the data packets evenly among nodes to avoid unwanted delay, overhead in network and the chance of attacks must be reduced by forming the network accordingly.

4. EVEN DATA DISTRIBUTION SCHEME

We have come up with an efficient even data distribution scheme to increase the packet delivery ratio in network and by decreasing the delay and overhead while transferring. In prior work, the data's are forwarded by considering the nodes performance and capacity. By doing so, the data packets are forwarded via only high performing nodes where other nodes are in idle state. The idle nodes are also using the energy which becomes waste. Due to dependence of only high performing node, there occurs delay and overhead in network. When the data packet stays for longer time in network, it pays a way for attackers or hackers to undergo malicious activities. To overcome the above mentioned issue, we prefer distributing the data evenly among the nodes in the selected route. It means that every nodes that are chosen are with same capacity and

produces similar performance. The nodes are chosen by considering their carrier power C_p, carrier sense C_s and the radius R_x. the algorithm that helps to distribute data event is hybrid data distribution algorithm, steps of this process is explained in algorithm 1

Hybrid Data Distribution Algorithm

Distributed algorithms are a traditional tool for protocol designing for sensor systems. Distributed algorithms are the theoretical forms that are used in distributed systems. Here we have studied and implemented how the nodes in the distributed network should be arranged for communication so that the data packets are transferred efficiently. This algorithm helps in sending the data evenly by analyzing the capacity and threshold limit of every network. With this implementation the packet delivery ratio to destination side is maintained evenly. The delay, overhead are maintained minimum in our system by forwarding the data based on even data distribution scheme. The proposed algorithm for even distribution of data among the nodes is to increase the PDR of the network substantially and decrease the delay and overhead. The algorithm is used to satisfy the following broad requirements:

- The algorithm should ensure evenness in the data transmitted among the sensor nodes in a network. Therefore the new algorithm must distribute data evenly efficiently across the sensor nodes. To achieve this, the capacity and performance of the nodes selected should be similar.
- The algorithm should improve the delivery ratio of the network considerably through uniform data dissipation.
- The algorithm should optimize the data distribution so as to avoid attacks during the data forwarding as well as avoid congestion.
- The algorithm should distribute the data packets evenly across all the sensor nodes, by efficient routing by considering the hop count in the network.
- The algorithm should employ the hybrid transmission technique.
- The algorithm should be simple so as to occupy the least memory space and be computationally fast.

Algorithm 1: Hybrid Data Distribution Algorithm
Initially M is in transit from pi to all its children in the spanning tree.
Code for pi:
1 when no message is received: // _rst computation event by pi
2 terminate
Code for pj , 0 · j · n ¡ 1, j 6= i:
3 upon receiving M from parent:
4 send M to all children
5 terminate

Routing by Hop count

In general the routing in networking is done by finding the shortest path from source to reach destination. In other words, it can also be said that depending on the hop count the path is identified. Routing is the vital process in networking to avoid delay, overhead or any malicious attacks. So in our proposed system also, routing is given much importance by implementing it with dijkstra's algorithm. The main thing to be considered is the hop count and how the algorithm is implemented. The brief of hop count and the dijkstra's algorithm is given in following sections.

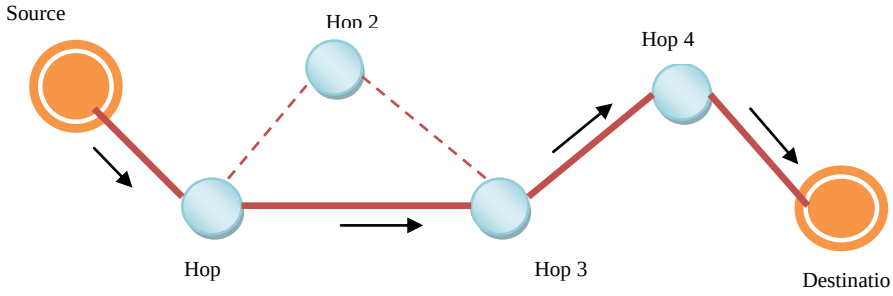

Figure 3. *Routing path chosen by Hop count*

Hop count

The term hop count in networking is number of transitional devices in total where the given data is passed between source and destination, rather streaming legitimately over a single wire. Every node in data path forms a hop, where the data moves from source to reach destination. The hop count is viewed as a fundamental estimation of distance in a network. And also it can be said that it provides approximate distance calculation between two given hosts. Hop count, n implies that an n gateway separates source and destination nodes.

Dijkstra's Algorithm

Generally, Dijkstra's algorithm is for discovering the shortest path among nodes in graph, which may represent, for instance, road systems. In the accompanying algorithm, the code u ← mindistance (Q,dist), looks for the mindistance u in minidistance set Q that has the least distance[u] value. w (u, v) restores the length of edge joining (for example the distance among) two neighboring nodes u & v. The variable distance[v] is the path length to neighbor node v from root node if it somehow happened to experience u. If this chosen path is short than the recorded current short path for v, that present path is supplanted with this dist path.

Algorithm 2:
distance[s]←0 //source vertex distance is 0
for all v ∈ V–{s}
do distance [v]←∞ //all other distances must be set to infinity
S←Ø //S, is initially empty which is set of vertices (visited)
Q←V //Q, initially the queue contains complete vertices
While Q ≠Ø //when queue is occupied, then
do u ← minidistance (Q,distance) //element of Q is select with minimum distance
S←S ∪ {u}//u is added to list of vertices (visited)
for all v ∈ neighbor [u]
do if distance[v] > distance[u]+w(u,v)
//when new shortest path is encountered
then d[v] ←distance[u] + w(u, v)
//set new shortest path;if need, traceback code can be added
return distance

Clustering
Clustering based on threshold is another strategy which automatically produces clusters dependent on threshold value. So this is utilized to improves chance of identifying the global ideal and not delicate to exception. Threshold value is set by considering various factors in network, they are, bandwidth of transmitting data, carrier power C_p, carrier sense C_s and the radius R_x.

5. SIMULATION RESULTS

In this section we analyze the data transmission among the nodes to analyze the overhead, delay and PDR of network by utilizing Network Simulator tool. The output obtained provides us with the result of delay and overhead in network and packet delivery ration when even transmission. The graph below (in figure 4) shows the variation in delay when the data is transmitted evenly among nodes in the network. The delay in the network is estimated by considering the time at which the packets are transferred. Here delay remains constant after some time where it ranges from 0 to 55 bytes and the time is calculated in seconds.

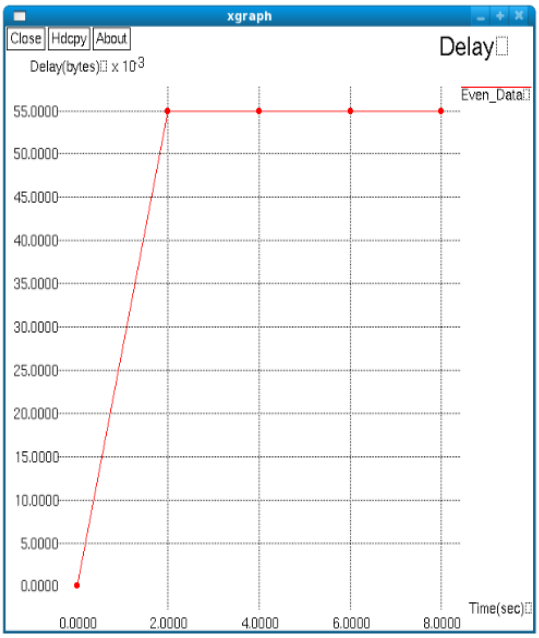

Figure 4. *Delay in network*

(X-axis: Time (sec), Y-axis: Delay (bytes) x 10^3)
Overhead in network occurs when the data packets remains in network for long time which must be reduced to avoid attack in network. Overhead is also measured with time that is measured in seconds. The overhead ranges from 5 to 6.3 bytes when even distribution (in figure 5).

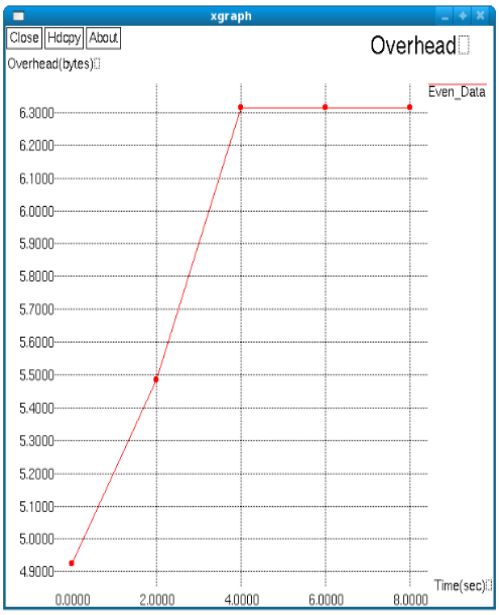

Figure 5. *Overhead in network*

(X-axis: Time (sec), Y-axis: Overhead (bytes))
Packet delivery ratio is the number of packets that is received as such at the destination. To know the performance of the network PDR helps greatly. If the data sent by source is received completely at destination then the PDR increases the performance of the network. The PDR is maintained constant even when the time increases where the delivery ratio is 0.95% (in figure 6).

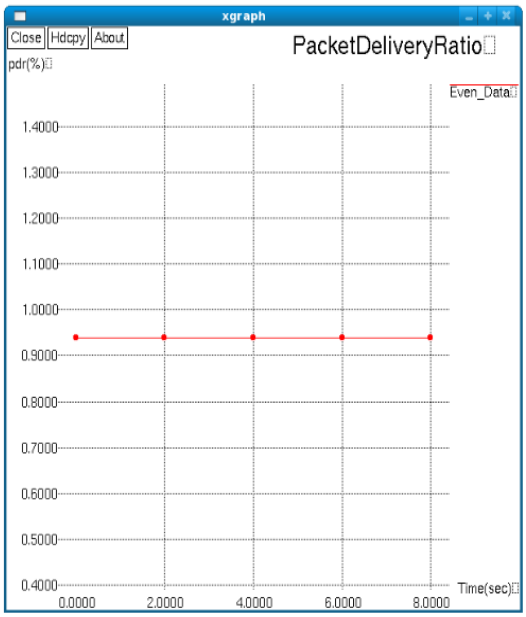

Figure 6. *Packet Delivery Ratio in network*
(X-axis: Time(sec), Y-axis: PDR(%))

6. CONCLUSION

We introduced a hybrid approach of data distribution for WSN in which the data's are sent to destination so that the packets are distributed evenly among the selected nodes. This is done with the help of the hybrid data distribution algorithm where the nodes with same capacity are selected by considering their carrier power, carrier sense and the bandwidth of the data to be sent are also considered. Routing path is found by considering minimum hop count in the network with dijkstra's algorithm. Then clustering is done by considering the threshold limit I_{thr} and the data packets are forwarded to destination. The proposed scheme decreases the overhead and delay that occurs due to forwarding of packets via high performing nodes. This in turn increases the PDR in network thus maintaining the performance of network. From the simulation results, the parameters estimated are delay, overhead and PDR which is illustrated as graph in previous section. In future, we intend to consider the composite event which takes multiple attributes into an account.

REFERENCES

[1] Manshahia, M. S. (2016). Wireless sensor networks: a survey. International Journal of Scientific & Engineering Research, 7(4), 710-716.

[2] Zhang, A.-L., Wang, G.-C., & Li, Y.-Z. (2012). WSN Multi-hops Routing Algorithm Based on Levels. 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control.

[3] Guruprasanna, & Sujatha, M. R. (2016). A novel approach to avoid malicious attack to enhance network in WSN. 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT).

[4] Wei, Y., Mao, Y., Leng, S., & Huang, W. (2014). A low-overhead energy-efficient ARQ protocol for wireless sensor networks. China Communications, 11(10), 74–87.

[5] Yildiz, H. U., Temiz, M., & Tavli, B. (2015). Impact of Limiting Hop Count on the Lifetime of Wireless Sensor Networks. IEEE Communications Letters, 19(4), 569–572.

[6] Cho, B. S., Lee, J., & Park, H.-K. (2014). Routing algorithm using channel based hop counting for wireless ad-hoc networks. 16th International Conference on Advanced Communication Technology.

Related work

[7] Ren, Y., Oleshchuk, V., & Li, F. Y. (2010). A Scheme for Secure and Reliable Distributed Data Storage in Unattended WSNs. 2010 IEEE Global Telecommunications Conference GLOBECOM 2010. doi:10.1109/glocom.2010.5683089

[8] Khan, M. F., Felemban, E. A., Qaisar, S., & Ali, S. (2013). Performance Analysis on Packet Delivery Ratio and End-to-End Delay of Different Network Topologies in Wireless Sensor Networks (WSNs). 2013 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Networks.

[9] Cheng, W., Li, Y., Jiang, Y., & Yin, X. (2014). A novel secure and repairable scheme for distributed data storage in unattended WSNs. 2014 9th IEEE Conference on Industrial Electronics and Applications.

[10] Cheng, W., Li, Y., Jiang, Y., & Yin, X. (2015). Secure data distribution scheme with two-hop survival strategy for unattended WSNs. International Journal of Distributed Sensor Networks, 11(10), 712598.

[11] Al-Karaki, Jamal N., and Ahmed E. Kamal. "Routing techniques in wireless sensor networks: a survey." IEEE wireless communications 11, no. 6 (2004): 6-28.

[12] Wei Ye, Heidemann, J., & Estrin, D. (n.d.). An energy-efficient MAC protocol for wireless sensor networks. Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies.