International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

Improving Reliability & Performance of WSN via Routing Errors

Anjila Daheriya, Rishi Sing kushwah, Kailash Patidar
Computer science & engineering Department
Sri Satya Sai Institute of Science and Technology, Sehore, India

Abstract- Wireless sensor networks have recently received increased attention for a broad array of applications such as surveillance, environment monitoring, medical diagnostics, and industrial control. A wireless sensor network (WSN) is a self-organized network that consists of a large number of low-cost and low powered sensor devices, which can be deployed on the ground, in the air, in vehicles, on bodies, under water, and inside buildings. The reliability of individual links' performance is crucial in these applications, e.g., in a surveillance network, the transmissions must be reliable to avoid false alarms and missed detections. We propose a scheme which automatically detect faulty link and discover secure shortest path for data transmission. The key is used for secure data transmission. In large-scale wireless sensor networks, damaged link detection plays a critical role in network diagnosis and management. The backup route cache is fetched from the backup node to check link damage failure. This message is used by backup node to replace the contents of data packet. This packet is used to inform all the nodes about route changes in the network. After getting the message source node S directs the packets with new and secured node. Our protocol ensures that multicast data is delivered from the source to the members of the multicast group, even in the presence of link failure, as long as the group members are reachable through non-adversarial path. We proposed Trust key computing, secure node authentication, and secure route discovery across the node to detect and secure data transmission. Experimentally result showed that our scheme is well suited for better data transmission.

Keywords- Faulty Link, Routing, Route Discovery, Security, Wireless Sensor Network.

I. INTRODUCTION

Wireless ad hoc network does not have any combined server but is a distributed, self-governing of any pre-established substructure network.A wireless sensor network (WSN)[1] consists of many tiny sized sensor nodes that have computation power, communication capability, and sensing functions. Each sensor node[1] can sense physical phenomena, like temperature, vibration, light, electromagnetic strength, humidity, and so on, and transmit the sensed data to the sink node through a chain of multiple intermediate nodes that help forward the data. Wireless sensor networks (WSNs) have received significant attention in recent years due to their potential applications in military sensing, wildlife tracking, traffic surveillance, health care, environment monitoring, building structures monitoring, etc. The most significant benefit of sensor networks is that they extend the computation capability to physical environment where human beings cannot reach. They can operate for prolonged periods in habitats that are hostile, challenging or ecologically too sensitive for human visitation, Moreover it has the potential to provide wealth of data about the environment in which they are deployed and send their results across the network to the end-users. Wireless Sensor Networks (WSNs) have been the preferred choice for the design and deployment of next generation monitoring and control systems. It has now become feasible to deploy massive amounts of low-cost sensors to monitor large regions over ground surface, underwater, or atmosphere. WSNs can be treated as a special family of wireless ad hoc networks. A WSN is a self-organized network [2] that consists of a large number of low-cost and low powered sensor devices, which can be deployed on the ground, in the air, in vehicles, on bodies, under water, and inside buildings. Each sensor node is equipped with a sensing unit, which is used to capture events of interest, and a wireless transceiver, which is used to transform the captured events back to the base station, called sink node. Sensor nodes collaborate with each other to perform tasks of data sensing, data communication, and data processing. Compared to the wired networks, it seems much more essential to detect link faults [2] rather than node faults in WSNs. A wireless link itself virtually exists, which means we can't directly observe and assess whether it performs well or not. It proves difficult to localize [3] the faulty links under a dynamic mal-condition in the wild, for the link quality will be significantly impacted by the natural environment like trees in the forest and flow in the ocean. Faulty link detection becomes more difficult in the multi-hop networks due to topology features. Faulty link detection plays an important role in network failure detection and network management. Link failure is one of the problems against wireless sensor networks and can affect the whole sensor network communication. The variety of technique against fault link detection is overwhelming. Because of the challenges of designing of routing protocols of wireless sensor network we have many constraints. WSN have limitations due to resources. WSN have low storage capacity, low bandwidth. The other limitations are low central processing unit and limited battery energy.The rest of the paper is organized as follows. Section 2 concentrates on the literature survey. Section 3 provides the proposed work and proposed algorithm. Section 4 provides the implementation and result analysis of proposed work. Finally, Section5 provides concluding remarks, limitation discussion.

II. LITERATURE SURVEY

A wireless sensor network is which organized itself according to the situation. It is a collection of nodes. The nodes are low cost and low battery power sensor devices. WSN can be positioned on the ground, in the air. It can be positioned in vehicles, on bodies of the human or animals. It can be deployed under water, and inside the houses. The main components of wireless sensor networks are sensing unit, and a wireless transceiver. The function of sensing unit is capture events of attention. The main function of wireless transceiver is transforming the captured events back to the base station. The base station is called sink node. Sensor nodes cooperate with every other to achieve tasks of data identifying, data communication, and data processing. In WSNs serious incident data collected [4] by the sensor nodes necessity to be reliably delivered to the sink for successful monitoring of an environment. The greatest noteworthy advantage of sensor networks is that they increased the computation ability to physical atmosphere where human beings cannot reach. They can work for lengthy periods in locales that are antagonistic, challenging or environmentally too sensitive for human examination. Moreover it has the probable to send prosperity of data about the setting in which they are organized and send their outcomes across the network to the users. A sensor node is a tiny component that is proficient of computation, sensing and communication competences. Sensor node is the main component of WSN. Sensor nodes can be used to sense moisture and temperature. It is also used to sense temperature and light. Since a single sensor transports only limited information; a system of these devices is used to achieve huge surroundings. The communication component in sensor nodes is used to transfer information. It has now become possible to install enormous quantities of low cost sensors to monitor big regions over ground underwater, surface, or atmosphere. WSNs have received noteworthy consideration in current years due to their potential applications in wildlife tracking, armed sensing, traffic investigation, fitness care, atmosphere monitoring, building constructions monitoring, etc. Nodes in WSNs are disposed to letdown due to hardware letdown, energy reduction, communication link faults, mischievous attack, and so on. The main WSN objectives are low node cost, small node size, low power consumption, scalability, self-configurability, better channel utilization, fault tolerance, adaptability, Qos [5] support and security. A wireless link itself virtually exists, which means we can't directly observe and assess whether it performs well or not. It proves difficult to localize the faulty links under a dynamic mal-condition in the wild, for the link quality will be significantly impacted by the natural environment like trees in the forest and flow in the ocean. Multi-hop networks suffer more harm than single- hop networks due to link failures. For example, a critical link may cause a large area of partition, or significantly interfere with routing protocol among the nodes, producing problems such as routing cycle and even network partition. Accordingly, compared to single-hop networks, faulty link detection becomes more difficult in the multi-hop networks due to topology features. A packet has to traverse multiple links to the sink, it is for this reason that exactly localizing a faulty link becomes really hard if only on the basis of whether the packet arrives at the sink or not. Therefore, faulty link detection becomes one of the most critical issues in multi-hop network diagnosis. According to the status of a link, packet loss failure, routing failure, partition can be found easily. Notably, link performance actually reflects a network's reliability and bottleneck if exist. Routing in wireless network is different from simple adhoc network. Wireless sensor network is infrastructure less. Wireless links are not reliable. All the routing protocols of wireless sensor network require good energy. Wireless sensor node may fail because of infrastructure. The wireless sensor network protocols are location based protocols, hierarchical protocols, data centric protocols, multipath based protocols, QoS based protocols, mobility based protocols, and heterogeneity based protocol. Although single link failures are more common, multiple link failures occur due to shared risks such as failure of a link while another link is under maintenance, or natural disasters that cause links traversing a region to fail. In [6], the authors use monitoring paths and cycles to localize single link and Shared Risk Link Group (SRLG) failures. They also prove that $(k+2)$ -edge connectivity was necessary and sufficient to uniquely localize all SRLG failures involving up to k links with one monitor. In practice, however, not all sensor networks can satisfy this strict condition, especially in the cases we spread the sensor nodes randomly in the area of interest. In addition, in most cases we are not allowed to set any more monitors after the deployment. What we expect is to utilize the rule-free probes (i.e., without computing the exact probing paths) to achieve link scan. One of the most peculiar routing characteristics of WSN is routing dynamics. It is not surprising that a sensor node frequently changes its parent to forward packets. Unfortunately, many existing approaches just aim to detect the faulty links which had been behaving badly, but fail to offer an inspection on other unused ones, thus have no guidance to reroute when the current routing strategy is less than satisfactory. To solve the above problems, in this work we propose Link Scanner (LS) [1], a passive and rule-free detection approach for discovering faulty links in sensor networks. The object of LS is to provide a blacklist containing all possible faulty links. With such a blacklist, further analysis and recovery processes become possible, including (i) exploring the root causes of observed symptoms in the network, (ii) adjusting routing strategy for the related nodes, (iii) offering the spare list of links for every node. As a result, we not only achieve the goal of diagnosis, but also take a big picture of wholly link performance. To maintain a sensor network running in a normal condition, many applications in flooding manner are necessary, such as time synchronization, reprogramming, protocol update, etc. In the flooding process, each node is expected to receive multiple probe messages through different paths. By embedding lightweight data into the flooding packet, LS passively collects hop counts of received probe messages at sensor nodes. Since faulty links may cause probes dropped, there must be mismatches between the received hop counts in sensor nodes and our expectations according to the topology. With a probabilistic and heuristics based inference model, LS analyzes the mismatches and deduces the faulty links. A wireless network often contains a large number of links which virtually exist in the air, but can never directly observe whether they perform well or not. Proposes a passive and low-cost link scanning scheme LS for faulty link detection. LS infers all links statuses on the basis of data collection from a prior probe flooding process, in which leverage hop count to reflect the in/out-going link performances. In the inference model, use to describe the inner relationship among the links, and finally output the optimal fault report with some constraints, which reversely generates a feedback for DLP's next computation. The algorithm through a test bed consisting of 60 TelosB sensor motes and an extensive simulation study, while a real outdoor system is deployed to links including those potential but not used ones in sensor networks. Item According to the exceptional features of sensor networks develops an efficient investigation marking scheme that exposes the innermost dependencies of sensor networks. Link scanner proposes characterized implication models to get the multi-level dependences between the network elements and accomplish great precision. Further introduce a learning-based inference scheme which increases the inspection accuracy and is thus scalable for large scale networks. A field study on a real outdoor deployment is also presented to verify that LS is practical to surveillance networks. Network diagnosis has been extensively studied in recent years. Existing approaches can be broadly divided into two categories: debugging tools and inference schemes. This work belongs to the latter category. Authors [7] is used a notable tool which focuses on debugging sensor nodes at the source-level, and enables developers to wirelessly connect to a remote sensor and execute debugging commands. Declarative Trace points [8] allow the developers to insert a group of action-associated checkpoints at runtime, which are programmed in an SQL-like declarative language. Existing inference-based diagnosis schemes for WSNs like trust deeply on an add in procedure that occasionally reports a big amount of network information from separate sensor nodes to the sink, announcing enormous overhead to the resource forced and traffic sensitive sensor network. In order to minimize the overhead, some researchers propose to establish inference models by marking the data packets and then parse the results at the sink to infer the network status, or conduct the diagnosis process in local areas. [9] Apply Belief Network with the bipartite graph to represent dependencies among links and end to end connections, then the root causes can be deduced by conducting inference on the Belief Network. [10] Explores the bottleneck nodes in a WSN, and [10] enhances the network visibility by analyzing the events and status in history. Besides, most approaches actively design their probes to fetch desired information for faulty link detection [9], especially in the managed enterprise WLANs and wireless mesh networks, where the monitors are easy to deploy. For each cycle, a node is required to monitor the cycle's performance. [7] Develops a non-adaptive fault diagnosis through a set of probes where all the probes are employed in advance. The authors in [9] propose a failure detection scheme, in which monitors are assigned to each optical multiplexing and transmission section. These approaches usually compute the probe paths according to different network symptoms, so as to combine the network topology to infer the link status. For a large scale sensor network, however, deploying monitors in the wild not only increases the cost, but also needs to guarantee sustainable management. Sniffers can be used to collect the information.

III. PROPOSED WORK

During flooding processes link scanner passively collects hop counts of received probe messages at sensor nodes. In wireless sensor networks, faulty link discovery [4] plays a serious role in network analysis and organization. The object of link scanner is to provide a blacklist containing all

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

possible faulty links. Based on the surveillance that damaged links can result in disparity between received hop counts and network topology with such a blacklist, further analysis and recovery processes become possible, including (a) discovering the root causes of observed indications in the network, (b) altering routing policy for the related nodes, (c) contribution the spare list of links for every node. Our procedure guarantees that multi cast data is transported from the source to the associates of the multi cast groups, even in the presence of link letdown, as long as the group members are accessible through non adversarial track. In order to detect faulty link, we proposes a scheme which help in report to the system. And also find path to secure data transmission. We evaluate the secure value of each node to select a protected track for message forwarding to identify the damaged and malicious nodes which are supposed to launch connection letdown.

Here authentication framework is used to remove outside adversaries and guarantee that only approved nodes accomplish certain operation.

3.1 Proposed Method

Step 1: Apply flooding process in a wireless sensor network

Step 2: Link scanner infers all links statuses on the basis of data collection from a prior probe flooding process.

Step 3: The next step is to count no of hops.

Step 4: If any mismatched in hop count then

Link failure detected and report to the system

else

select backup node with authentication

end if

Step 5: Generation of secure key in which node initialization time is taken as a secure key

After getting the secure key the node is marked as authenticated node.

Step 6: Check whether node have secure key then authentication successful for data transmission and node is marked as secure node.

Step7: The next step is to find route for secure data transmission. The shortest path is discovered across the node.

Step 8: Select a node to destination

If selected node is found in route_list then

Selected node is marked as secure node and route discovery is successful. Route is confirmed for data transmission

Else

Select another new node, check authentication

End if

Step 9: During data transmission any link may fail so backup node selection mechanism is always used by system for backup node setup.

Step 10: After successful data transmission the route record is maintained by system for future use.

Table 1 Simulation parameter

Quantity of nodes	50, 100, 150, 200
Simulated area dimension	510×710
Routing Procedure	LEACH
Simulation time seconds	90
Transport Layer	TCP with FTP protocol
Traffic flow type	CBR
Packet size in bytes	1010
Quantity of traffic links	20 , 8
Max. Speeds in m/s	30

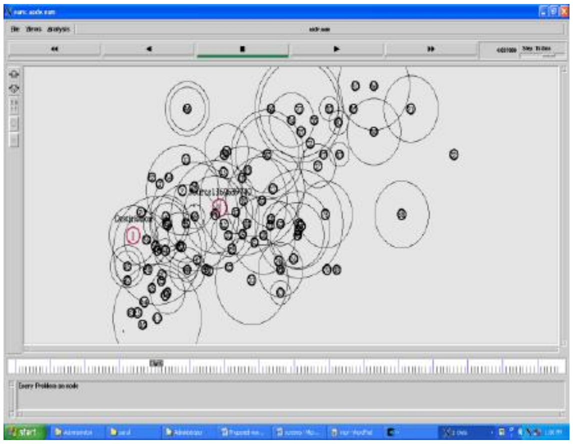

Figure 1Topology generated with secure key generation.

Figure 2 No of nodes and average packet delivery ration

IV. IMPLEMENTATION

We used Network Simulator 2 simulator software for implementation of our proposed algorithm. The methodologies we used are improved faulty link detection and data transmission algorithm to improve the performance of wireless sensor network. We also used C/C++ and TCL language for implementation. We

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

performed our experiment in Intel i3 4.0 GHz machine with 2GB RAM. Given Figure shows the average data packet delivery delay for each level node in a fixed area with fixed number of nodes using multilevel scheme. As the level increases, the delay also increases. But since our protocol tries to minimize the number of levels so the delay is also reduced as compared to other multihop protocols.

V. CONCLUSION

In large-scale WSNs, damaged link discovery plays a serious role in network diagnosis and administration. Secure data transmission regardless of link failure is also essential condition for huge establishments. The proposed scheme automatically find damaged link which may break the communication and determine protected shortest path for data transmission. We evaluate the trust data of each node to select a protected path for message forwarding to find the malicious nodes which are supposed to launch connection letdown. Our procedure guarantees that multicast data is delivered from the source to the associates of the multicast cluster, even in the presence of connection letdown, as long as the group associates are accessible through non adversarial path. We proposed Trust value calculating, protected node verification, and secure route finding across the node to find and secure data transmission. Experimentally outcome showed that our scheme is well suitable for improved and protected data transmission. We are planning to implement our work with wireless sensor node localization in surveillance environment. A direction of future investigation with decent probable is improving the quality of routing tree. It proves problematic to localize the damaged links below an active mal condition in the remote, for the link excellence will be meaningfully impacted by the natural atmosphere like plants in the forest and movement in the marine.

REFERENCES

[1]. Qiang Ma, Kebin Liu, Zhichao Cao, Tong Zhu, Yunhao Liu, Link Scanner: Faulty Link Detection for Wireless Sensor Networks, IEEE Transactions On Wireless Communications, Vol. 14, pp. 4428-4438, Aug 2015

[2]. S. S. Ahuja, S. Ramasubramanian, and M. M. Krunz, “Single-link failure detection in all-optical networks using monitoring cycles and paths,” IEEE/ACM Transaction Network, vol. 17, no. 4, pp. 1080–1093, Aug. 2009.

[3]. Q. Cao, T. Abdelzaher, J. Stankovic, K. Whitehouse, and L. Luo, “Declarative trace points: A programmable and application independent debugging system for wireless sensor networks,” in Proc. ACM SenSys, Raleigh, NC, USA, pp. 85–98, 2008.

[4]. A. Cerpa, J. L. Wong, L. Kuang, M. Potkonjak, and D. Estrin, “Statistical model of lossy links in wireless sensor networks,” in Proc. IEEE IPSN, 2005,PP. 81-88.

[5]. H. Chang et al., Spinning beacons for precise indoor localization,” in Proc. ACM SenSys, Raleigh, NC, USA, pp. 127–140, 2008.

[6]. W. Dong, Y. Liu, Y. He, T. Zhu, and C. Chen, “Measurement and analysis on the packet delivery performance in a large-scale sensor network,” IEEE/ACM Transaction Network, vol. 22, no. 6, pp. 1952–1963, Dec. 2014.

[7]. L. Girod et al., “Em-Star: A software environment for developing and deploying wireless sensor networks,” in Proc. USENIX Annu. Technical Conference Boston, MA, USA, 2004.

[8]. Y. Hamazumi, M. Koga, K. Kawai, H. Ichino, and K. Sato, “Optical path fault management in layered networks,” in Proc. IEEE GLOBECOM, Sydney, NSW, Australia, , pp. 2309–2314, 1998.

[9]. N. J. A. Harvey, M. Patrascu, Y. Wen, S. Yekhanin, and V. W. S. Chan, “Non-adaptive fault diagnosis for all-optical networks via combinatorial group testing on graphs,” in Proc. IEEE INFOCOM, Anchorage, AK, USA, pp. 697–705, 2007.

[10]. N. Leone et al., “The DLV system for knowledge representation and reasoning,” ACM Trans. Computer Logic, vol. 7, no. 3, pp. 499–562, PP. 1430–1440, 2006.