International Journal of Advanced Technology & Engineering Research (IJATER)
www.ijater.com

LINK LETDOW DETECTION AND IMPROVING RELIABILITY IN WIRELESS SENSOR NETWORK

Harpreet Kaur[1], Dr. Sumit Saghwan[2], Gurpreet Singh[3]
Electronics & Communication Department[1,2,3]
Ganga Institute of Technology and Management, Kablana Haryana [1,2,3]

Abstract:

The main objectives are design of WSN low node cost, small node size, low power consumption, scalability, self configurability, better channel utilization, fault tolerance, adaptability, Qos support and security. Nodes in WSNs are disposed tolet down due to hardware letdown, energy reduction, communication link faults, mischievous attack, and so on. The main objective of the proposed work is to detect damaged link from WSN, determine route for protected data transmission and improve the performance and reliability of network.

Key Words: wireless sensor network, data transmission, Communication capability.

Introduction

Wireless ad hoc network does not have any combined server but is a distributed, self-governing of any pre-established substructure network.A Mobile Adhoc Network (MANET)[1] is a gathering of wireless nodes that can dynamically be set up anytime and anywhere without using any pre-existing network arrangement. AODV[2] is, as the name suggests, a distance vector routing protocol. It is also used for other wireless ad-hoc networks. Ad hoc On-Demand Distance Vector (AODV). The nodes in the network are themselves responsible for routing the packets from the source to the destination. It is a widely used routing protocol for mobile ad hoc networks (MANETs). These nodes are also responsible to make the transfer of packets secure. AODV is an approach able routing set of rules i.e.it founds a source to an endpoint only on request. In dissimilarity, the widely used routing protocols of the WWW are proactive, i.e. they find routing track autonomously of the usage of the paths.

Wireless sensor networks establish a specific type of wireless data communication networks. A wireless sensor network (WSN)[3]contains of numerous small sized sensor nodes that have computation power. It also has communication ability and sensing functionalities. Every sensor node can sense physical characteristics. WSNs have been the favorite choice for the succeeding generation monitoring and control systems. It can sense temperature, light, vibration, electromagnetic strength, humidity, and so on, and transmit the sensed data[3] to the sink node through a chain of multiple intermediate nodes that help forward the data.

Wireless sensor networks (WSNs) have been widely used in many application areas such as infrastructure protection, environment monitoring and habitat tracing. 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. Compared to the wired networks, it seems much more essential to detect link faults rather than node faults in WSNs. Declarative Trace points [2], 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 Sympathy [17] or Emstar [6] 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.

Besides, most approaches actively design their probes to fetch desired information for faulty link detection [1], 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. [8] develops a non-adaptive fault diagnosis through a set of probes where all the probes are employed in advance. The authors in [7] propose a failure detection scheme, in which monitors are assigned to each optical multiplexing and transmission section.

Wireless Sensor Network

The main WSN objectives are low node cost, small node size, low power consumption, scalability, self configurability, better channel utilization, fault tolerance, adaptability, Qos support and security. Nodes in WSNs are disposed toletdown due to hardware letdown, energy reduction, communication link faults, mischievous attack, and so on. 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 design challenges of WSN are limited energy capacity, sensor locations, limited hardware resources, massive and random node deployment, network characteristics and unreliable environment, data aggregation, diverse sensing application requirements, scalability.

Proposed Methodology

In wireless sensor networks, faulty link discovery plays a serious role in network analysis and organization. During flooding processes link scanner passively collects hop counts of received probe messages at sensor nodes. Based on the surveillance that damaged links can result in disparity between received hop counts and network topology. The object of link scanner is to provide a blacklist containing all possible faulty links. 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.

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. Then to select a protected track for message forwarding to identify the damaged and malicious nodes which are supposed to launch connection letdown.

Our procedure guarantees that multicast data is transported from the source to the associates of the multicast groups, even in the presence of link letdown, as long as the group members are accessible through non adversaril track.

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

Proposed Procedure Contains Subsequent Stages

(1) Link scanner infers all links statuses on the basis of data collection from a prior probe
flooding process, in which hop count to reflect the in/out-going link performances.

(1) Trust key computing

(2) Secure node authentication

(3) Secure route discovery across the node.

(4) Backup node setup phase.

(5) Route maintenance across the node.

Algorithm

.Select a node to destination

Check selected node in fresh route cache

If yes then
Route is confirmed
Else
Select another new secured node
End if

Trust Key value Calculations

The first steps in algorithm is trust key value calculation. A novel parameter weight value named TLv can be used to select the finest track which guarantees reliability of the path by calculating the belief value of the adjacent nodes and that value can be stored in a precedence table of the scheme. Every time a node sends a route request either when it determines that it should be a part of a multicast groups, and it is not already a member of that group, or when it has a message to send to the multicast group but does not have a route to that group. An in-between node after receiving a route request packet updates its path in the routing table and add the TLv value of its link and forward it to the next node.

To estimate the belief value a new trust strategy has been introduced in our proposed work. The trust value is introduced in network and link layer of WSN. The dynamic assignment of weight is introduced in the network to compute a key which can be used to determine the consistency of neighbor node.

To calculate the trust value a new trust policy has been introduced in link and network layer to calculate a key which can be used to determine the reliability of neighbor node, where the key calculation involves dynamic assignment of weights.

The strategy exist in in route entry trust computing part. It functions independently and preserves its separate viewpoint of trust hierarchy. It collects all the information about the neighbors. The information includes control packet and data packet and overheads data of neighbors. The information may contain dumped and not retransmitted packet detail of the neighbors.

Based on this information each node maintain some useful values in a table for its all neighbor’s nodes.

Table 1: Trust Value Table

Destination	Next Hop	Interface	TSTv
3	3	2	4
2	2	8	3
8	4	5	2
5	2	6	5
6	4	8	7

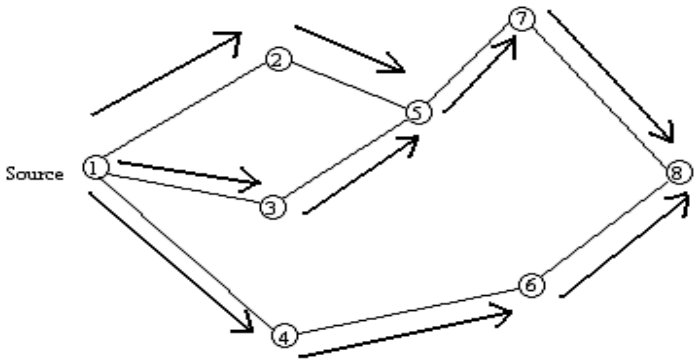

Figure 1. Wireless sensor network with source node 1.

Simulation Results and Analysis

Network Simulator-2 (Ns) is a widely used network simulator for network related research work. NS (version 2) is an object-oriented, network simulator developed at Berkely. It is written in C++ and OTcl (Tcl script language with Object-oriented extensions developed at MIT). NS offers considerable provision for simulation of TCP and UDP. It is also used in routing, and multicast procedures over wired and wireless networks.The NS mission is now a part of the VINT project. NS also implements media access layer protocols for LAN. NS project develops tools for simulation results. NS is primarily useful for simulating LAN and WAN.

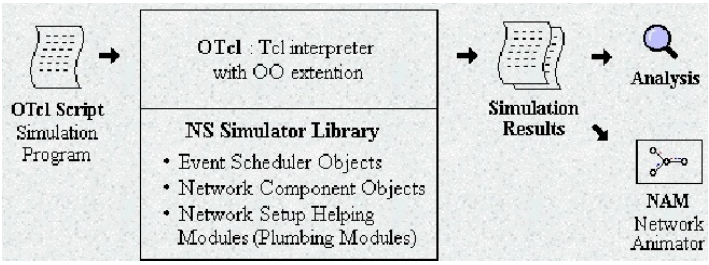

Figure 2 Simplified view of NS2

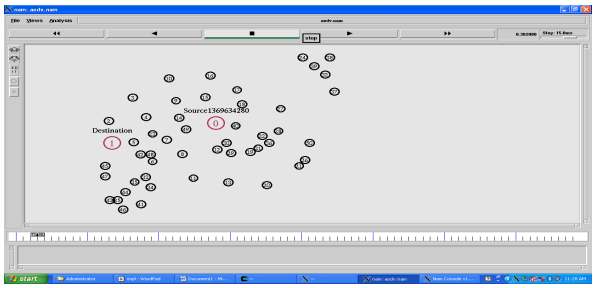

Figure 3 A sample topology generated by ns-2 fifty Node Case

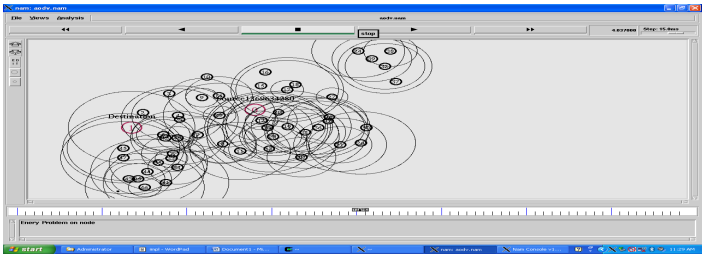

Figure 4: A sample Topology generated by ns-2 fifty Node case with data transmission

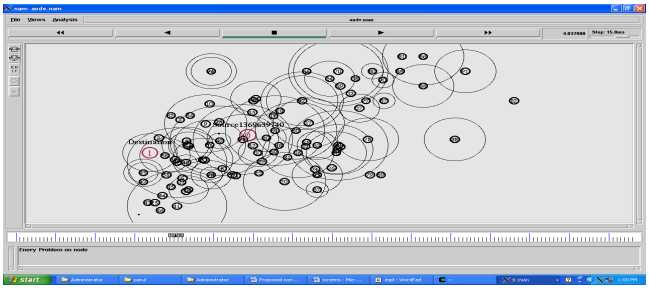

Figure 5: A Sample Topology generated by NS-2 with faulty node

Conclusions

WSNs have recently received increased consideration for a comprehensive collection of applications such as investigation, atmosphere monitoring, health diagnostics, and industrial control. 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.

In this concern, the thesis set out with essential objective to find damaged link and protected data transmission. 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 adversrial 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.

References

[1] T. S. Rappaport et al., Wireless Communications: Principles and Practice, vol. 207, Englewood Cliffs, NJ, USA: Prentice-Hall, 1996.

[2] 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 Trans. Netw., vol. 22, no. 6, pp. 1952–1963, Dec. 2014.

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

[4] 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

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

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

[7] 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.

[8] L. Girod et al., "EmStar: A software environment for developing and deploying wireless sensor networks," in Proc. USENIX Annu. Tech. Conf., Boston, MA, USA, 2004, p. 24.

[9] 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, 1998, pp. 2309–2314.

[10] 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, 2007, pp. 697–705.

[11] N. Leone et al., "The DLV system for knowledge representation and reasoning," ACM Trans. Comput. Logic, vol. 7, no. 3, pp. 499–562, Jul. 2006.

[12] X. Li, Q. Ma, Z. Cao, K. Liu, and Y. Liu, "Enhancing visibility of network performance in large-scale sensor networks," in Proc. IEEE ICDCS, Madrid, Spain, 2014, pp. 409–418.

[13] Z. Li, Y. Liu, M. Li, J. Wang, and Z. Cao, "Exploiting ubiquitous data collection for mobile users in wireless sensor networks," IEEE Trans.Parallel Distrib. Syst., vol. 24, no. 2, pp. 312–326, Feb. 2013.

[14] Y. Liu et al. Does wireless sensor network scale? A measurement study on greenorbs," in Proc. IEEE INFOCOM, Shanghai, China, 2011, pp. 873–881.

[15] Y. Liu, K. Liu, and M. Li, "Passive diagnosis for wireless sensor networks," IEEE/ACM Trans. Netw., vol. 18, no. 4, pp. 1132–1144, Aug. 2010.

[16] Q. Ma, K. Liu, X. Miao, and Y. Liu, "Sherlock is around: Detecting network failures with local evidence fusion," in Proc. IEEE INFOCOM, Orlando, FL, USA, 2012, pp. 1430–1440.

[17] Q. Ma, K. Liu, T. Zhu, W. Gong, and Y. Liu, "BOND: Exploring hidden bottleneck nodes in large-scale wireless sensor networks," in Proc. IEEE ICDCS, Madrid, Spain, 2014, pp. 399–408.