Dynamic Multi-Hop

Mr. Amey Maskawadkar[1] Mrs. Sukeshni Gawai[2] Mr. Onkar Naram[3] Mr. Samiksha More[4] Mr. Akshata Botre[5]
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]Dr.D.Y.Patil Polytechnic , Akurdi Pune, India

Abstract— Multi-hop routin is where cluster heads close to the base station functionaries as intermediate nodes for father cluster heads to relay the data packet from regular nodes to base station. Building such a backbone requires efficient clustering algorithms which aggregate network nodes into logical groups, each group being managed by a cluster head and any two neighboring clusters being interconnected by at least one gateway node or gateway path. In this concept G-hop clustering refers to cluster structures where cluster members are at most G hops away from their cluster head. Where as the dynamicity of mobile wireless network is often considered as the biggest challenge, in this work we explicitly exploit node mobility in order to support cluster formation and maintenance of G-hop clusters. Many protocols have been emerged for facing the problem of energy consumption in the wireless sensor network (WSN). Low Energy Adaptive Clustering Hierarchy (LEACH) protocol is one of those protocols, which achieves a lot of spreading though. In this paper, dynamic multi-hop technique (DMHT-LEACH) protocols have been proposed based on the LEACH protocol.
Key words: Routing, Network Topology, Topology, Wireless Sensor Networks, Wireless Communication, Vehicle Dynamics, Routing Protocols

I. INTRODUCTION

In a multi-hop sensor network, the origin of data allows the BS to trace the source and forwarding path of an individual data packet. Origin must be recorded for each packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of sensor nodes. Therefore, it is necessary to devise a solution with low overhead.

We formulate the problem of secure data transmission in sensor networks, and identify the challenges specific to this context. We propose an in-packet BF data-encoding scheme. We design efficient techniques for data decoding and verification at the base station. We perform a detailed security analysis and data evaluation of the proposed technique. Our design is efficient techniques for data decoding and verification at the base station. We extend the secure data encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes. We perform a detailed security analysis and performance evaluation of the proposed data encoding scheme and packet loss detection mechanism. We only require a single channel for both transmission channels for data and origin.

A. User Classes and Characteristics

1) Sender

The sender(source) will send the message i.e. data packets by data encoding scheme and send to destination via intermediate nodes.

2) System

Our system detects automatic packet drop(by low bandwidth, frequency, etc factors),or packet drop by hacker, with the help of bloom filter

a) Assumptions and Dependencies

1) There should be active sensor nodes to transmit for transmission of data.
2) The system should run in windows operating system

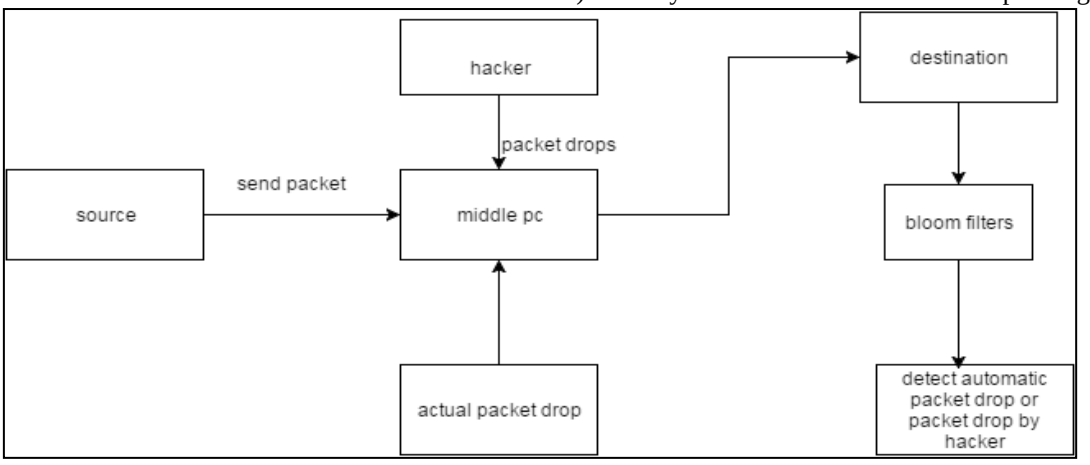

Fig. 1: User Classes and Characteristic

II. REQUIREMENTS

A. External Interface Requirements

1) User Interfaces

The GUI (Graphical User Interface) needs to be provided which is user friendly to interact with the system. User will send the message or data packets to destination through the intermediate nodes.

2) Hardware Interfaces

There should be required devices to interact with software.

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.

- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 256 Mb.

3) Software Interfaces

There has to be required packages, software's etc to interact with system.

- Operating system: Windows XP Professional/7LINUX.
- Coding language: JAVA/J2EE.
- IDE : eclipse kepler

B. Functional Requirements

1) Data Encoding

For a data packet, data encoding refers to generating the vertices in the graph and inserting them into the iBF. Each vertex originates at a node in the data path and represents the data record of the host node.

2) Data Decoding

a) Data Verification:

When the BS receives a data packet, it executes the pdata verification process, which assumes that the BS knows what the data path should be, and checks the iBF to see whether the correct path has been followed. However, right after network deployment, as well as when the topology changes (e.g., due to node failure), the path of a packet sent by a source may not be known to the BS.

b) Data Collection:

A data collection process is necessary, which retrieves provenance from the received iBF and thus the BS learns the data path from a source node. Afterwards, upon receiving a packet, it is sufficient for the BS to verify its knowledge of origin with that encoded in the packet

III. Conclusion

Our proposed DSA-DMRP is a dynamic multi-hop routing protocol using unequal sized clustering approach. This protocol is based on the modified KHOPCA rules by adding a priority factor. The priority factor is a parameter for selecting the CHs in the network that consider the residual energy and distance to the BS. The fuzzy aggregation technique is used to measure the data similarity degree of adjacent nodes. The DSA-DMRP was compared against the KHOPCA to justify the performance. The DSADMRP and the KHOPCA have an approximately same stability of alive nodes. However, The DSA-DMRP can reach a longer the network lifetime than the KHOPCA in all terms of FND, HND, and LND. Therefore, the DSA-DMRP can extend the network lifetime in a relatively significant manner and can satisfy the requirement of multi-hop routing protocol for dynamic node clustering based on the data similarity of their neighbors.

References

[1] Dousse, O., Thiran, P. and Hasler, M. Connectivity in Ad hoc and Hybrid Networks. City, 2002.
[2] Santi, P. Topology Control in Wireless Ad Hoc and Sensor Networks. Wiley, 2005.
[3] Peleg, D. Distributed computing: a locality-sensitive approach. Society for Industrial and Applied Mathematics Philadelphia, PA, USA, 2000.
[4] Luo, H. G., Ye, F. G., Cheng, J. G., Lu, S. G. and Zhang, L. G. TTDD: Two-Tier Data Dissemination in Large-Scale Wireless Sensor Networks. Wireless Networks, 11, 1 2005), 161-175.
[5] Zhu, S., Setia, S. and Jajodia, S. LEAP: efficient security mechanisms for large-scale distributed sensor networks. Proceedings of the 10th ACM conference on Computer and communication security2003), 62-72.
[6] Basagni, S. Distributed and mobility-adaptive clustering for multimedia support in multi-hop wireless networks. City, 1999.
[7] Andronache, A., Brust, M. R. and Rothkugel, S. Multimedia Content Distribution in Hybrid Wireless using Weighted Clustering. ACM Press, City, 2006.
[8] Dow, C.-R., Lin, J.-H., Hwang, S.-F. and Wang, Y.-W. An Efficient Distributed Clustering Scheme for Ad-hoc Wireless Networks. IEICE Trans. Commun., E85-B, 8 2002).
[9] Nocetti, F. G., Gonzalez, J. S. and Stojmenovic, I. Connectivity Based k-Hop Clustering in Wireless Networks. Telecommunication Systems, 22, 1-4 2003), 16.

