IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 1, Ver. III (Jan - Feb. 2015), PP 05-08
www.iosrjournals.org

Cooperative Data Forwarding In AODV Routing Protocol

Sarath Menon[1] Mr. Jose Anand [2]
KCG College of Technology, Karapakkam, Chennai - 600097.

Abstract: *A Wireless sensor Network uses thousands of miniature devices that communicate among each other and sense data from the environment. The success of the communication in a WSN inherently lies in the routing protocol used by the architecture. This work enables reliable communication for Reactive Routing Protocol such as, Ad hoc On-demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) in Wireless Sensor Networks. These protocols are on-demand routing protocols and has the capability to only detect Link Failures. This hampers the packet delivery ratio and increases the end-to-end delay. AODV Protocol when faced with a link failure condition has the source node reinitiate the route discovery phase by broadcasting Route Request Messages to its neighbours without considering the affected link. The system calls for a Reliable Reactive Routing Enhancement (R3E) as an extension over the AODV protocol. Here the nodes maintain a list of forwarding candidates and their priorities with the help of routing table enabling forwarding of data towards destination as per node priority and thereby removing the need for re-initiation of route discovery phase. Thus R3E successfully augments the aforementioned AODV protocol, thereby improving the packet delivery ratio and also achieving a significant reduction in end-to-end delay in the Wireless Sensor Network.*

Keywords: *Wireless Sensor Networks, Ad-Hoc On Demand distance Vector, Dynamic Source Routing, Link Failure.*

I. Introduction

Wireless Sensor Networks

Wireless Sensor Networks (WSN) can be defined as a computer network consisting of thousands of miniature devices capable of computation, communication and sensing data from its environment. They represent the next big step in creating the smart environment. The success of the smart environment depends on the sensory data and hence the WSN's. They provide a bridge between the physical and virtual worlds. The challenges in the hierarchy of detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays and performing decision-making and alarm functions are enormous.

II. Components In Wireless Sensor Networks

The Fig 1.1 shows the various components in the WSN. Typically WSNs contain hundreds or thousands of sensor nodes, and these sensors have the ability to communicate either among each other or directly to an external base station (BS). A greater number of sensors allows for sensing over larger geographical regions with greater accuracy. Basically each sensor node comprises sensing, processing, transmission, mobilizer, position finding system, and power units (some of these components are optional, like the mobilizer). Sensor nodes are usually scattered in a sensor field, which is an area where the sensor nodes are deployed. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment. Each sensor node bases its decisions on its mission, the information it currently has, and its knowledge of its computing, communication and energy resources. Each of these scattered sensor nodes has the capability to collect and route data either to other sensors or back to an external BS(s). A BS may be a fixed or a mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data.

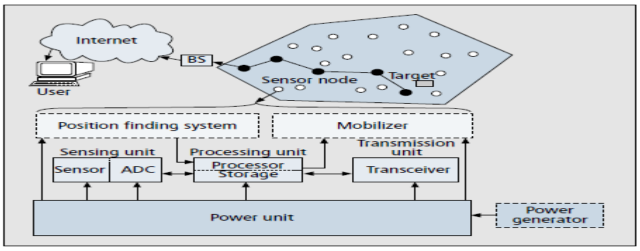

Fig 1.1 Components in WSN

III. Routing In Wsn

Routing in WSNs is very challenging due to the inherent characteristics that distinguish these networks from other wireless networks like mobile ad hoc networks or cellular networks. First, due to the relatively large number of sensor nodes, it is not possible to build a global addressing scheme for the deployment of a large number of sensor nodes as the overhead of ID maintenance is high. Thus traditional IP-based protocols may not be applied to WSNs. Furthermore sensor nodes that are deployed in an ad hoc manner need to be self-organizing as the ad hoc deployment of these nodes requires the system to form connections and cope with the resultant nodal distribution, especially as the operation of sensor networks is unattended. In WSNs sometimes getting the data is more important than knowing the IDs of which nodes sent the data. Second in contrast to typical communication networks almost all applications of sensor networks require the flow of sensed data from multiple sources to a particular BS. This however does not prevent the flow of data to be in other forms (e.g., multicast or peer to peer). Third sensor nodes are tightly constrained in terms of energy, processing and storage capacities. Thus they require careful resource management. Fourth in most application scenarios nodes in WSNs are generally stationary after deployment except for maybe a few mobile nodes. Nodes in other traditional wireless networks are free to move which results in unpredictable and frequent topological changes. However in some applications some sensor nodes may be allowed to move and change their location (although with very low mobility). Fifth sensor networks are application-specific. Sixth position awareness of sensor nodes is important since data collection is normally based on the location. Finally data collected by many sensors in WSNs is typically based on common phenomena, so there is a high probability that this data has some redundancy. Such redundancy needs to be exploited by the routing protocols to improve energy and bandwidth utilization. Usually WSNs are data centric networks in the sense that data is requested based on certain attributes.

IV. Existing System

Ad Hoc On Demand Distance Vector Routing is the most prominently used reactive routing protocol in wireless sensor networks. This protocol has the ability to detect only the link failure condition in the network. Link failure conditions are detected by the absence of HELLO messages between the neighbour nodes in the network. Thus in case of link failure condition in the network the source node again reinitiates the route discovery phase by flooding the network with Route request packet. This hampers the throughput and the packet delivery ratio (PDR), while the end to end delay is also on the ascendancy.

V. Proposed System

The system calls for augmenting the existing AODV routing protocol with a concept of Reliable Routing Reactive Routing (R3E). This concept is used as an extension to the AODV routing protocol which enables the network to bypass the link failure condition. Thereby during a link failure condition the source node greedily progresses the data towards the destination using the guide path. Thus there is no need for the source node to re- initiate the route discovery phase in case of link failure. This increases the throughput, packet delivery ratio (PDR) while reducing the end to end delay in the network.

Reliable Reactive Routing Enhancement (R3E)

The project proposes an idea of R3E which is used as an extension over the AODV protocol. This enhances the AODV routing protocol to provide reliable and energy efficient packet delivery against the condition of Link Failure which may occur in a wireless sensor network.

Fig 1.2 shows the functional architecture overview of R3E. It is a middle-ware design across the MAC and the network layer. The R3E enhancement layer module consists of three main modules. They are Reliable Route discovery module, potential forwarder selection and prioritization module and forwarding selection module. The reliable route discovery module finds and maintains the route information for each node. The other two modules are responsible for the runtime forwarding phase. Forwarding decision module will check whether the node receiving a packet is one of the intended receivers if it is true then the node will cache the incoming packet. The potential forwarder selection and prioritization module attaches the ordered forwarder list in the data packet header for the next hop. Lately the outgoing packet will be submitted to the MAC layer and forwarded towards the destination.

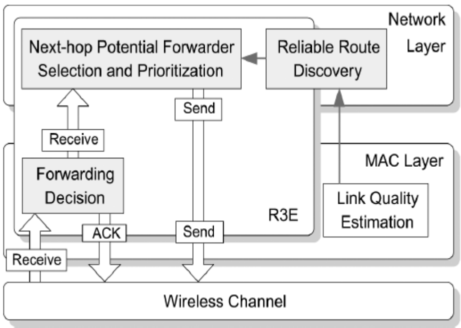

Fig 1.2 Functional Architecture overview of R3E

AODV-R3E Implementation

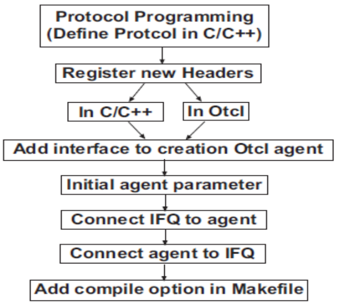
Protocol Programming (Define Protcol in C/C++)
Register new Headers
In C/C++
In Otcl
Add interface to creation Otcl agent
Initial agent parameter
Connect IFQ to agent
Connect agent to IFQ
Add compile option in Makefile

Fig 1.3 AODV-R3E Implementation

Fig 1.3 shows the steps followed to implement the R3E protocol over the AODV Routing Protocol. Creation of c/c++ files in the folder is the primary step in this process. Modifying the files in NS2 is done so that the system can recognize the R3E protocol in the simulation. Registration of packet header is done in c++ so that the simulator will recognize the above idea. Modification of the existing AODV protocol is done. Modification is done with the existing header files and there is a need to add some extra header files as well which will take care of the node priority TTL expiration cases and routing table updation. Connection of interfacing queue and routing agent to each other is essential. Last step is to add new compile options to the “Make- file” and rebuild the NS2 software.

AODV-R3E

R3E is implemented with the AODV routing protocol to achieve AODV-R3E. It acts along with the AODV routing protocol and enhances its resilience to the condition of link failure. Source Node wishes to send data to the destination node. It first checks its routing table to find the neighbouring nodes and broadcasts RREQ packets to them. The intermediate node then broadcasts the RREQ packet to downstream nodes. This is done till the packet reaches the destination node or the node that is one hop path away from the destination. This node sends Route Reply packet to the source node through the intermediate nodes. A Source node will get many Route Request packets. It will accept one of them and will reject all others. The data forwarding will happen along the way that was traversed by the Route Reply packet. In case a link failure occurs in the network which is indicated by profound drop in packets or the absence of beacon signals in the network. In the above case the source node refers to its routing table and will forward the packet to the next preferable neighbour nodes and in this way the packet from the source to destination will reach without using the broken link and without undergoing the process of Route discovery again. This can happen as long as the data forwarding is between the same source- destination pair. In case some other node wants to send the data towards a destination node it should be done only after Route discovery phase.

VI. Results And Analysis

The reliable Reactive Routing Enhancement (R3E) is implemented over the AODV routing protocol. Simulation is carried out in NS-2.29 for two cases namely

1) Link failure condition in AODV Routing Protocol.
2) Link failure condition in AODV-R3E Routing Protocol.

It is seen that in case of the link failure condition in the network AODV-R3E greedily progresses the data towards the destination as opposed to the AODV Routing Protocol. AODV- R3E does not have the source node reinitiate the route discovery phase in the above scenario. While for AODV Routing Protocol Route discovery phase is an essentiality in case of link failure condition in the network.

Comparison

Simulation was done for the above scenarios. The Graph was plotted for 3 parameters throughput, packet delivery ratio and end to end delay taken in y-axis vs increasing node density taken on x axis. The comparison is given in the form of a table given below.

Parameters	AODV	AODV-R3E
Throughput	0.9Mbps	5.5 Mbps
End to end delay (Min)	20 ms	12 ms
Packet delivery ratio	90%	100%

VII. Conclusion

The Proposed R3E protocol served as an efficient Protocol acting as an extension to the AODV Routing protocol as figuratively indicated by the Table. It increased the resilience of the network against the condition of link failure. It reduced the end to end delay and did appreciably well in increasing the Throughput and the Packet delivery Ratio as compared with the aforementioned Ad hoc On Demand Routing Protocol.

Future Work

The future work will focus on introducing the Concept of Intrusion detection System (IDS) by implementing the idea of Enhanced Adaptive ACKnowledgement(EAACK).This system will focus on ideas to protect the network from malicious attack of the nodes in the network itself. Thus it will make the network robust against any intruder that may be encountered by the network.

References

[1]. Vehbi Cagri, Gungor, Özgür B. Akan and Ian F. Akyildiz, (April 2008), “A Real-Time and Reliable Transport (RT)^2 Protocol for Wireless Sensor and Actor Networks”, IEEE Trans. Networking,Vol.16,No.2, pp. 359-370.

[2]. X. Huang, H. Zhai, and Y. Fang, (Dec 2008), “Robust cooperative routing protocol in mobile wireless sensor networks”, IEEE Trans. Wireless Commun., Vol. 7, No. 12, pp. 5278–5285.

[3]. Xufei Mao, Shaojie Tang, Xiahua Xu, Xiang-Yang Li and Huadong Ma, (Nov 2011), “Energy Efficient Opportunistic Routing in Wireless Sensor Networks”, IEEE Trans. Parallel and Distrib. Syst., Vol. 22, No. 11, pp 1934-1942.

[4]. Jianwei Niu, Long Cheng, Yu Gu, Lei Shu and Sajal K. Das, (Feb 2014), “R3E: Reliable Reactive Routing Enhancement for Wireless Sensor Networks”, IEEE Trans. Industrial informatics, Vol.10, No.1, pp. 784-794.

[5]. Eric Rozner, Jayesh Seshadri, Yogita Ashok Mehta and Lili Qiu, (Dec 2009) “Soar: Simple opportunistic adaptive routing protocol for wireless mesh networks”, IEEE Trans. Mobile Comput., Vol. 8, No. 12 pp. 1622–1635.

[6]. Elhadi M. Shakshuki, , Nan Kang and Tarek R. Sheltami, (March 2013), “EAACK—A Secure Intrusion-Detection System for MANETs”, IEEE Trans Industrial Electronics, VOL. 60, NO. 3, pp 1089-1098.