International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 3 Issue 1 January 2016

A Network lifetime Enhancement method for sink Relocation and its Analysis in Wireless Sensor Networks

Suma khan[1], Pankaj Kawadkar[2]
Dept of Computer Science & Engineering, Patel College of Science & Technology, Bhopal, India[1]
Professor, Dept of Computer Science &Engineering, Patel College of Science &Technology, Bhopal, India[2]
ksuma8010@gmail.com[1], kawadkarpankaj@gmail.com[2]

Abstract: -*The Wireless Sensor Network (WSN) is an emerging field for the researches in the current scenario. Transferring data from source node to destination is the most important task in the wireless sensor network. The Mobile nodes also have limited battery power which is a challenge for node to long time survival in network. Main drawback for the any wireless sensor networks is limited energy available to nodes because of the small size of the batteries they use as source of power. Balancing the route of the data transfer is one of the techniques that can be used to minimized sensor nodes energy consumption during operation. Life of network is directly proportional battery power in mobile nodes. This dissertation presents an algorithm that reduces the power consumption by using energy efficient routing over sensor network.The technique has been tested through simulations for different distributions of nodes. Under all the evaluated scenarios, the technique demonstrates excellent performance as compare to existing one. The simulation shown the ESAODV achieves substantial energy efficiency which indicates that ESAODV outperforms several previously proposed protocols like LEACH, PEGASIS and BCDCP*
.

Keywords: - *Wireless Network, Sensor Network, Proactive Routing protocols, Reactive Routing protocols, Hybrid Routing Protocols, mobile ad hoc.*

1. INTRODUCTION

The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. Through advanced mesh networking protocols, these devices form a sea of connectivity that extends the reach of cyberspace out into the physical world. As water flows to fill every room of a submerged ship, the mesh networking connectivity will seek out and exploit any possible communication path by hopping data from node to node in search of its destination. While the capabilities of any single device are minimal, the composition of hundreds of devices offers radical new technological possibilities.

The power of wireless sensor networks lies in the ability to deploy large numbers of tiny nodes that assemble and configure themselves. Usage scenarios for these devices range from real-time tracking, to monitoring of environmental conditions, to ubiquitous computing environments, to in situ monitoring of the health of structures or equipment. While often referred to as wireless sensor networks, they can also control actuators that extend control from cyberspace into the physical world.

A Network is use to connect the devices for sending and receiving the data. To install any network there are three basic needs. These are 1) Computers 2) Connecting Media and 3) Protocol. As the network is a way to provide communication between two or more than two devices. Whether, wireless network uses radio waves to connect devices such as laptops to the Internet and to your business network and its applications. When you connect a laptop to a WiFi hotspot at a cafe, hotel, airport lounge, or other public place, you're connecting to that business's wireless network. Using this approach the wireless LAN can create to establish it in a required area[1].The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance, an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a

wireless network ad hoc and infrastructure. Earlier there was a discussion that Wireless network refers to a network, in which all the devices communicate without the use of wired connection. Wireless networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves; for the carrier and this implementation usually takes place at the physical level or "layer" of the network [2].

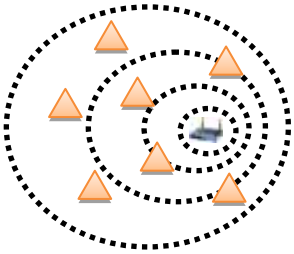

Figure 1.1: Wireless Network

Figure 1.1 shows the Wireless network, which have very limited bandwidth and are relatively less reliable due to environmental effects in comparison of wired network that provide plentiful bandwidth and reliable links in wired networks.

Sensor Network - Sensor networks are dense wireless networks of small, low-cost sensors, which collect and disseminate environmental data. Wireless sensor networks facilitate monitoring and controlling of physical environments from remote locations with better accuracy.

They have applications in a variety of fields such as environmental monitoring, military purposes and gathering sensing information in inhospitable locations. Sensor nodes have various energy and computational constraints because of their inexpensive nature and ad-hoc method of deployment.

Applications of Sensor Network- Sensor networks have a variety of applications. Examples include environmental monitoring, which involves monitoring air soil and water, condition based maintenance, habitat monitoring (determining the plant and animal species population and behavior), seismic detection, military surveillance, inventory tracking, smart spaces etc. In fact, due to the pervasive nature of micro-sensors, sensor networks have the potential to revolutionize the very way we understand and construct complex physical system.

Sensor Network and Protocols

2. SENSOR NETWORK ROUTING

Routing in sensor networks involves finding a path from the source to the destination, and delivering packets to the destination nodes while nodes in the network are moving freely [3]. Due to node mobility, a path established by a source may not exist after a short interval of time. To manage with node mobility nodes need to maintain routes in the network. Depending on how nodes establish and maintain paths, routing protocols for ad-hoc networks broadly fall into pro-active, reactive, hybrid, and location-based categories.

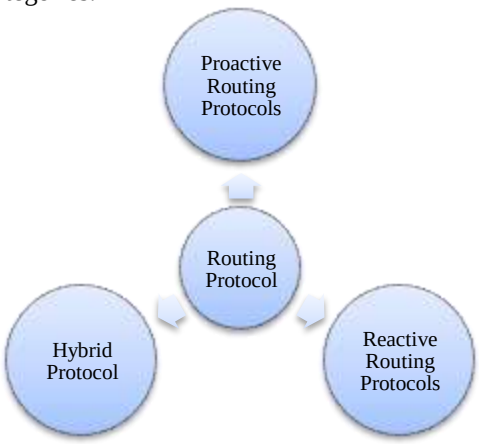

Figure 2.2 Protocol Used in sensor network

AD-HOC ON DEMAND DISTANCE VECTOR ROUTING

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network [4]. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected

set of nodes to be notified so that they are able to invalidate the routes using the lost link.

One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes [5]. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number

Ad hoc On-Demand Distance Vector, AODV is a distance vector routing protocol is reactive. Property reactive routing protocol means it requires a route when you need one and does not require that mobile nodes maintain routes to destinations that are not reported [6, 7]. AODV provides loop-free paths using sequence numbers that indicate how new or fresh, it is a path. [8] [9] [10]. The AODV protocol is a protocol for order routing for ad-hoc networks that are being developed by the Ad-hoc mobile networks (MANET IETF) group.it work follows the approach of distance vector routing instead of origin. In AODV, everynode maintains a local routing table that contains the information to the neighbors, to transmit a data packet to finally reach the desired destination. It is generally desirable to use the paths have a length according to a skip count as the metric distance [9,11]. However, AODV provides functionality such as DSR, ie the transport of data packets from one node to another by finding the routes and taking advantage of the multi-hop communication. AODV is based on UDP as a transport protocol to deliver packets in disordered ad-hoc network. In addition, it requires that each node can be solved by a single IP address through the network and send packets properly by placing the IP address of the IP packets from the sender. It also means that AODV is designed to operate in a friendly network where security is less of a concern. It is worth mentioning that no extension of AODV tries to avoid malicious nodes to attack the integrity of the network by using digital signatures to ensure packet routing control [12]. AODV requires each node to maintain a routing table that contains an entry for each channel of the destination node is in communication with. Each route entry keeps track of certain fields. Some of these areas are:

A. **Destination IP Address**: The IP address of the destination for which a route is supplied.
B. **Destination Sequence Number**: The destination sequence number associated to the route.
C. **Next Hop**: Either the destination itself or an intermediate node designated to forward packets to the destination.
D. **Hop Count**: The number of hops from the Originator IP Address to the Destination IP Address.
E. **Lifetime**: The time in milliseconds for which nodes receiving the RREP consider the route to be valid.
F. **Routing Flags**: The state of the route; up (valid), down (not valid) or in repair.

3. NETWORK SIMULATOR

The proposed approach for detection of Wormhole attack is implemented using ns-2 by doing necessary modifications in the existing implementation of AODV such that "Modified AODV" detects wormhole attack while maintaining its normal functionalities. This chapter covers the details of implementation work and the necessary modifications in existing implementation of AODV.

This section deals with Network Simulator Version 2, also known as NS-2. NS-2 is an event driven packet level network simulator developed as part of the VINT project (Virtual Internet Testbed)[1]. This was a collaboration of many institutes including UC Berkeley, AT&T, XEROX PARC and ETH. Version 1 of NS was developed in 1995 and with version 2 released in 1996. Version 2 included a scripting language called Object-oriented Tcl (OTcl). It is an open source software package available for both Windows 32 and Linux platforms.ns (network simulator) is a name for the series of simulations of discrete event systems, particularly ns-1, ns-2 and ns-3. All are discrete event network simulator, used mainly in research [13] and teaching. ns-3 is free software, available to the public under the GNU GPLv2 license for research, development and use.

4. RELATED WORK

It has been seen that most of the previous approaches for chose alternate path directly when any node shutdown that dropped performance and have relative higher complexity. As the mobile nodes operate on the limited power of battery therefore it becomes very necessary to develop techniques which can successfully maintaining lesser complexity. The objective of this dissertation is to develop a new approach which can successfully maintain

the rout with lesser battery power in order to long survival of Sensor network.

Sensor network is a classification of wireless networks use to collect and disseminate environmental data having low-cost sensors. Wireless sensor networks facilitate monitoring and controlling of physical environments from remote locations with better accuracy. They have applications in a variety of fields such as environmental monitoring, military purposes and gathering sensing information in inhospitable locations. Sensor nodes have various energy and computational constraints because of their inexpensive nature and ad-hoc method of deployment.

Previous author shows that, in these types of network battery consumption is a changing issue. It is important that the node must be long time survival in the network. Due to dynamic changes there is major issue in this types of network.

5. PROPOSED METHODOLOGY

ESAODV is a proactive node disjoint multipath routing protocol. In ESAODV, WSN is assumed to consist of several steps Sti = 1, i 2, ..., l based on the number of hops between the source and destination. The sink is a node St0 zero. Each node can communicate with the receiver node is St1. We assume that a node can communicate with nodes on the same stage Sti and the next step + 1 but cannot communicate with Sti-1 nodes. This avoids looping paths. Initially, all network nodes have a very high value of the hop count with the exception of the receiving node. Initially, all nodes have their residence above the threshold energy level energy. Multiple paths from all nodes to the sink is generated in the construction phase of the road. In the process of building the packages Route (RCON) are exchanged between nodes. Each sensor node transmits the packet once RCON and maintains its own routing table. If there is no path to the sink node through the RCON received packet, then the node processes the packet RCON. If the path to flow from this node is already available in the routing table of the node, then the number of hops the packet is checked. If the hop number of packets is less than the value of the node and its residual energy jump is greater than the power threshold value, then it is RCON; otherwise the packet is discarded. The node receiving the RCON packet, updates the RCON packet. RCON is updated with incremental number of hops by one, updates the node ID before adding the node identifier in the way. The node receiving the RCON packet updates its routing table as the number of hops and path node to the receiver. Similarly, all nodes in the network receive the RCON packet and update their routing tables. Once they are all multiple paths are generated, the node disjoint multipath identified between the source and destination. When the source node to send the data from the target, extends the FFI trace data between nodes disjoint multipath based and long tail filled fill residual energy. If a path disjoint node fails due to the death of routing node movement or node, it informs the source node through the RERR packet.

6. PROPOSED ALGORITHM

Assumption

Ni = Node ID
Si = Sender ID
Ri = Receiver ID
Ei = Energy
Ti = Threshold Energy
Xi = Initial X location
Yi = Initial y Location

Algo( )

Node Si uses AODV Broadcast Route Request
{
If (Node exist in Range && Node Energy ≥ 10) // 10 Joule threshold value
{Received Route Packet
Match Ri ID to Self ID
If (Not Match)
{Initiate Ei of Node into Packet Header
Forward Packet to Next Hop
If(Ri ID = =Self Current Node ID)
{Receiver Found}
Check all Available Path from Si to Ri
Select Maximum Energy Path
}
Else if (Node Energy ≥ 10) // 10 Joule threshold value
{

- Ri broadcast position replacement packet search node having higher node energy…
- Each Neighbor node reply
- Select node with maximum energy and lowest distance apart

}
Else

{
Node not Found
}
}

7. RESULT ANALYSIS

Proposed ESAODV show better result in term of packet delivery ratio, battery power consumption and control packet overhead.

- **Packet Delivery Ratio: -** The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. The Proposed ESAODV having higher packet delivery ratio as compare with EENDMRP. EENDMRP has higher degree packet loss. Figure 5.13 shows the comparative study of the packet delivery ratio. By the graph it is clear that the packet delivery ratio is good by the proposed approach.

Figure 5.13 Packet Delivery Ratio of Proposed Protocol

- **Control packet overhead: -**packet overhead known as a time it takes to transmit data on a packet-switched network. Each packet requires extra bytesof format information that is stored in the packet header, which, combined with the assembly and disassembly of packets, reduces theoverall transmission speed of the raw data. For any ideal routing protocol it is required that it has lower control packet overhead, whereas existing EENDMRP have required higher control packet as compare to proposed ESAODV.

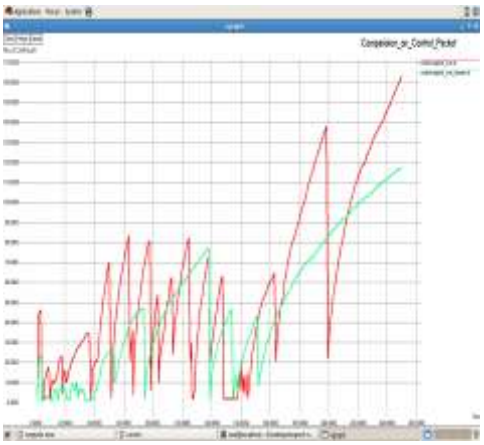

Figure 5.14 Control Packet Overhead

As far as the graph is concert it shows the comparative study of the Proposed Protocol and Existing Protocol. The red line shows the previous approach results and green line shows the proposed approaches result. It is clearly shown that the control packet overhead is less by the proposed methodology.

- **Battery Power Consumption:-**The energy consumption rate in a wireless sensor network significantly changes with respect to the protocols used for sensors. Here thesensors are going to use in order to perform the communications. There are various factors like voltage required for the operation; transmission power, received power etc are responsible to calculating the lifetime of a sensor node. Towards Energy saving routing protocol proposed protocol try to move lower energy node towards less traffic and higher energy node towards high traffic and reduce retransmission whereas existing approach only minimized redundant path.

Figure 5.15 Battery Power Consumption

8. CONCLUSIONS

This work has proposed the ESAODVProtocol for multipath energy efficient routing over sensor network. This method encapsulate advantage of two different predefine method in order to overcome their limitation. First one is alternate path and second one is clustering approach.

The technique has been tested through simulations for different distributions of nodes. Under all the evaluated scenarios, the technique demonstrates excellent performance as compare to existing one.The simulation shown theESAODV achieves substantial energy efficiencywhich indicates that ESAODV outperforms several previously proposed protocols like LEACH, PEGASIS and BCDCP.

REFERENCES

[1]. ZunnunNarmawala, Sanjay Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks" in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2008.
[2]. Sheikh, R. Singh Chande, M. and Mishra, D.K., "Security issues in MANET: A review", pp 1-4, IEEE 2010.
[3]. Ren Yueqing, Xu Lixin A study on topological characteristics of wireless sensor network based on complex network", pp486 – 489,IEEE 2010.
[4]. P. Papadimitratos and Z. J. Haas, "Secure Routing For Mobile Ad Hoc Networks" in Proc. of CNDS, 2002.
[5]. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, "A Secure Routing Protocol For Ad Hoc Networks" in Proc. of IEEE ICNP, 2002.
[6]. R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks In Wireless Networks Using Connectivity Information" in Proc. of IEEE INFOCOM, 2007.
[7]. Ali Modirkhazeni, SaeedehAghamahmoodi, ArsalanModirkhazeni and NaghmehNiknejad, "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", pp 122-128.IEEE 2011.
[8]. Fei Shi, DongxuJin, Weijie Liu and JooSeok Song, "Time-based Detection and Location of Wormhole Attacks in Wireless Ad Hoc Networks", pp 1721-1726,IEEE 2011.
[9]. Ronggong Song, Peter C. Mason and Ming Li, "Enhancement of Frequency-based Wormhole Attack Detection", pp 1139-1145,IEEE 2011
[10]. Kordafshari, M.S.;Pourkabirian, A.; Faez, K.; Rahimabadi, A.M., "Energy-Efficient SPEED Routing Protocol for Wireless Sensor Networks", PP 267-271,IEEE 2009
[11]. S. A. Razak, S. M. Furnell and P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols", School of Computing 2004.
[12]. Rong Cui; ZhaoweiQu ; Sixing Yin, "Energy-efficient routing protocol for energy harvesting wireless sensor network", pp 500 – 504,IEEE 2013.
[13]. Verma, M.K. andJoshi, S. ; Doohan, N.V. "A survey on: An analysis of secure routing of volatile nodes in MANET", pp 1-3, IEEE 2012.