Cooperative and secured Data Forwarding in AODV Routing Protocol

Sarath Menon [1], Mr. Jose Anand [2]
PG Scholar, Dept. Of ECE, KCG College of Technology [1]
Associate Professor, Dept. Of ECE, KCG College of Technology [2]

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 is an extension to include security aspects and also to further increase the routing parameters. The Earlier work enabled reliable communication for Ad hoc On-demand Distance Vector Routing (AODV) in Wireless Sensor Networks. The problem was that These protocols are on-demand routing protocols and has the capability to only detect Link Failures. This would hamper the packet delivery ratio and increases the end-to-end delay. AODV Protocol when faced with a link failure condition had the source node reinitiate the route discovery phase by broadcasting Route Request Messages to its neighbours without considering the affected link. This work calls for an EAACK concept as an extension over the AODV-R3E protocol.. The Idea Of Enhanced Adaptive Acknowledgement improves the security aspects of the wireless sensor networks. Thus EAACK successfully augments the aforementioned AODV-R3E protocol, thereby still improving the packet delivery ratio and also achieving a significant reduction in end-to-end delay in the Wireless Sensor Network.

Keywords: WSN, AODV, DSR, Link Failure, EAACK.

I. Introduction

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. WSN Components

. 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

ISSN: 2278 – 909X

sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data.

III. Security in WSN

The primary goals of security in WSN are to provide:

- **Confidentiality** – Data being transported in the network cannot be read by anyone but only the intended recipient.
- **Integrity**– Any message received is known to be exactly the message that was sent, without additions, deletions or modifications of the content.
- **Authenticity** – A message that claims to be from a given source is, in fact, from that source. If time is used as part of the authentication scheme, authenticity also protects a message from being recorded and replayed.

IV. 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.

V. 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. so The idea of Reliable Reactive Routing enhancement (R3E) provided the AODV routing protocol a mean to bypass the link failure scenario which was not possible in the case of the

ISSN: 2278 – 909X

AODV Routing Protocol. Thus in case of link failure condition in the network the source node need not reinitiates the route discovery phase by flooding the network with Route request packet. This enhances the throughput and the packet delivery ratio (PDR), while the end to end delay is also on the ascendancy compared to these parameters for AODV routing protocol.

VI. Proposed System

The system calls for augmenting the existing AODV-R3E routing protocol with the idea of Enhanced Adaptive Acknowledgement (EAACK). This concept is used as an extension to the AODV-R3E routing protocol which enabled the network to bypass the link failure condition and also improve the security of the network. 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. Further more when the idea of EAACK Supplements R3E concept it takes care of the Security issues of the wireless sensor networks using the AODV routing protocol. This still increases the throughput, packet delivery ratio (PDR) while reducing the end to end delay in the network.

1) Reliable Reactive Routing Enhancement (R3E)

The system earlier proposed an idea of R3E which was used as an extension over the AODV protocol. This enhanced 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. This amalgamation was discussed in the earlier work. It was 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.

2) Enhanced Adaptive Acknowledgement (EAACK)

The concept of Enhanced Adaptive Acknowledgement is an idea that embodies three core ideas given as below

I) Acknowledgement (EAACK)

Acknowledgement is an End to End acknowledgment scheme. The destination node sends an acknowledgement to notify the sender node that the packet that was sent by the sender node through the intermediate node to the intended receiver is received without any mishappenings.

II) Secure Acknowledgement (S-ACK)

S-ACK mode is activated when the source node does not receive the acknowledgement from the destination node. The ideology behind Secure Acknowledgement is to let the three consecutive nodes to work as a group. The third node after receiving the packet is required to send an acknowledgement in the backward direction indicative of the fact that the third node in the group has received the packet being forwarded in its

ISSN: 2278 – 909X

direction towards the destination. If the first node in the group does not receive this ACK it will switch on to the MRA mode and this may indicate that the intermediate node is malicious or it has a limited transmission power.

III) Misbehaviour Report Authentication (MRA)

The Misbehaviour Report Authentication Mode is initiated to handle and detect the malicious nodes in the network. It is seen that the malicious nodes can easily drain the resources of the network. The principle behind the MRA mode is that the source node will look to forward the data towards the destination using the other route in the network that will not involve the suspicious nodes, these nodes are suspicious of being malicious. This begins with the source node looking its routing table and seeks an alternative routes towards the destination. Destination nodes will receive the MRA packet from the source node and sees whether the packet was already received, if it was then the report is declared non authentic and the node/s generating the report is declared malicious. Then this node may be moved out of the network and future packet forwarding will not involve these nodes. Hence the valuable resources are preserved in the network.

3) AODV-R3E-SACK Architecture

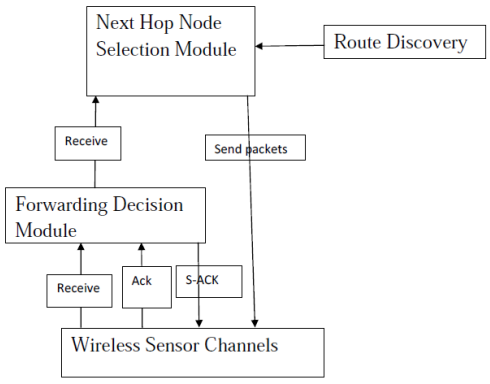

Fig 1 System Architecture of AODV-R3E-SACK

R3E is earlier 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. To improve the performance aspects of the network the idea of EAACK supplements the AODV-R3E. This is enabled by implementing the ideas of ACK, S-ACK and MRA. This provides the network with some sense of security and will further more decrease the average End to End delay. Throughput is also seen to be increased while there is no major loss in the packet delivery ratio (PDR). 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.

VII Results and Analysis

Simulation was carried out in Ns- 2.34. The Graph was plotted for 3 parameters

ISSN: 2278 – 909X

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	AODV-R3E-EAACK
Throughput(Mbps)	0.9	5.5	5.6
Avg. End to End delay (min)	20 ms	11 ms	9.5 ms
Packet delivery Rtio (PDR)	90%	100%	100%

VIII Conclusion

The Proposed EAACK protocol served as an efficient Protocol acting as an extension to the AODV-R3E Routing protocol as figuratively indicated by the Table. It increased the security of the network and also made the network resilient against the condition of link failure Meanwhile the concept of EAACK also supplemented the R3E idea well. Overall there was a reduction in 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.

IX Future Work

The future work could focus on introducing the Concept of Digital signature to make the network still more reliable and robust. This system will focus on ideas to protect the network from other prevelant attack of the nodes in the network itself. Thus it will make the network still more robust against any intruder that may be encountered by the network. Meanwhile there could still be an efficient use of the resource by the network and future work could concentrate on that aspect. This could still mean an increase in the throughput and an abnoscious decrease in the End to End delay.

REFERENCES

1) 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.

2) 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.

3) Jamal N. Al-Karaki Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey.

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) Rachit Jain and Lakshmi Shrivastava, (July 2011) "Study and Performance Comparison of AODV & DSR on the basis of Path Loss Propagation Models", International Journal of Advanced science and technology, Vol. 32, pp 45-52.

6) Rizwan pasha, (June 2010), "NS-2 Simulator Network simulator An introduction".

7) 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

ISSN: 2278 – 909X

Networks", IEEE Trans. Networking,Vol.16,No.2, pp. 359-370.

8) 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.

9) 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.

10) Yang Qin, Dijiang Huang and Bing Li, (Mar/April 2014) "STARS: A Statistical Traffic Pattern Discovery System for MANETS", IEEE Trans. Dependable and secure computing, Vol.11, No. 2, pp 181-192.

11) Zehua Wang, Yuanzhu Peter Chen, Cheng Li, "Implementation of the AODV Routing Protocol in ns2 for Multi-hop Wireless Networks".

ISSN: 2278 – 909X