DETECTING AND PREVENTING THE WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORK

P. Saranya\textsuperscript{1}, Abin P Varghese\textsuperscript{2}, R S Balaji\textsuperscript{3}
\textsuperscript{1}Assistant Professor, CSE Department, SRM University, Chennai
\textsuperscript{2,3}CSE Department, SRM University, Chennai

Abstract-A Wireless Sensor Network (WSN) is a collection of petite sensor terminals, capable of sensing and communication. Here topology is dynamic Node developments result in dynamic topology and cause link failures in an Ad-hoc. Here focusing on the using of packet scheduling technique for AODV (Ad Hoc on Demand Distance Vector) routing protocol by weight hop based scheduling in this paper. The transitional node starts the packet scheduling and manages its buffer memory according to data transfer rate. Intermediate store the data packets and repair the broken route and manage overflow of data packets. This proposed system attempt to send the data packet by utilizing backup routes opposed to dropping it. It evaluates the planned procedure on NS-2.34 simulator. Simulation results show that proposed scheme performance is better than AODV.

Keywords: Wireless networks, AODV, DSR, Wormhole, Wireless sensor networks.

I. INTRODUCTION

Wireless Sensor Network is an arrangement of remote portable nodes that progressively “self-categorize out in subjective and brief network topologies. Routing plays an important role in communication between nodes due to the dynamic character of nodes. Ad-hoc networks are classified into two reactive and proactive approaches depending on routing behavior routing protocols. In reactive routing protocols routes are determined only when they are required by a source node. Ad-hoc on Demand Distance Vector (AODV) \cite{8} routing protocol is a reactive routing protocol in which whenever a source node has data to send to some destination; it starts route discovery process by sending Route Request (RREQ) packet to its neighbors. If an intermediate node has a route entry corresponding to that destination, it sends a Route Reply (RREP) packet to the source else. AODV creates the next-hop entry for the reverse path to the source, to use when sending a reply -and then forward (broadcasts) message towards the destination. When RREQ" packet reaches the destination, it sends RREP packet to the source node by using reverse paths. If a source receives multiple replies, it selects the route with a lowest hop count. We know that AODV routing protocol uses the hop by hop routing, it uses the intermediate node for forwarding of data packets. In AODV, the intermediate node is responsible for the routing of packets, for route maintenance it sends the packet through the alternate path. In AODV, whenever a path breaks, it has to perform a route discovery which in turn increases contention and further increases overhead. In the packet networks, mobile node is admissible to use the resources such as buffer and link bandwidth. Here we focus on the packet scheduling of packet for efficient routing. We consider the AODV routing protocol for sending the packets. Dynamic Source Routing (DSR) \cite{7} uses the source routing, for this source node is responsible routing of packets. In DSR source node has the alternate path for route maintenance. DSR routing protocol uses the route salvaging process. A Recent survey on Multipath routing shows that disjoint path gives the best result for low mobility. Another, Split Multipath Routing (SMR) uses the disjoint path from the source node. Further, SMR enhancement for large area uses the route maintenance process according to a position of link break. In this project, we are using packet scheduling algorithm to provide the priority level for data packets. Scheduling of packet shows which packet to serve next and this process avoids
traffic, packet drop and simultaneously improves the performance. In our proposed technique we are using the weight hop based packet scheduling algorithm. For multi-hop network, each mobile node has the ability to share the link” with some restrictions.

II. RELATED WORK

A. CSMA-based wireless ad hoc networks using carrier sense threshold

Distributed Coordination Function is the MAC scheme that frequently used in IEEE 802.11, is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Though the CSMA/CA[1] is very effective and efficient, it can cause serious unfairness or flow deprivation in multi-hop wireless networks. This is a general MAC coordination problem due to the random access protocol using carrier sensing. In this paper, we give importance to propose algorithms to solve FIM (Flow-in-the-Middle) problem surrounded by deprivation problems. FIM occurs in situation a mid flow transmitter detects the outer flow transmitters which are not depended to each other. In order to reduce deprivation caused by FIM-like topology[1], we will implement an algorithm which is simple and efficient which adjusts carrier sense threshold heuristically. Moreover, we suggest an algorithm to make a node be aware of itself in FIM” situation.

B. Physical energy detection to recognize starvation in wireless networks

Carrier sense multiple access protocols entail stations, it desired to convey the initial check for the shared medium for the current transmissions. In wireless networks stations, it is not able to detect transmissions from all other stations in various locations. It also undergoes various amounts of contention[2], which tends to unfairness and starvation. Here, models the way of allocating the bandwidth for 802.11 MAC protocol for multiple saturated flows. Considered the definite class of topologies that has n independent flows, where each sender can sense k neighbors on” either side.

C. Rate, power and carrier-sense management

It is widespread for discovering wireless networks that are organized in the spontaneous manner. As of small hardware cost, to achieve good performance for large quantity of devices. Large quantity of devices is implemented in small space. Many disadvantages are available in sharing the medium. Here proposes a novel method that maintain rate of data, transmit power and carrier sense threshold to reduce the existing problem.

D. Modeling and identification of Starvation

The large number of deployed hotspots and home networks results in performance humiliation or even malnourishment[4]. Even the developing methods also lead to starvation. Here the analytical model categorizes the performance of data flow in wireless network. The novel method consumes the techniques from the working model and applies them in multi-hop wireless networks. It accounts for the MAC in multi-hop network, to handle varying power levels. Here, proposed a simple identification mechanism that determines the sources of starvation using local measurements.

E. Synchronous two-phase rate and power

Network ability and battery existence amplified by Adaptive transmit power control [5] in mobile devices. But it has some issues: 1) it aggravates the destination interference and irregular channel access; 2) it improperly tends to create data rate lower. 3) Variation in channel frequency is enhanced by mobility at small time scale. It reduces the problem complexity. Despite existing methodologies, there is no solution found to solve the problem. In this paper, we design and implement a synchronous two-phase rate and power control model which has dexterity in addressing the problems with efficient power control. Here uses Linux MadWifi driver that shown that it can analyses the hardware and do efficient power management, thereby fostering immediate deployability. Our extensive experimental evaluation on a real tested in an office environment demonstrates that: 1)
enables up to 80% of the clients in three different cells to settle at 50%–94% lower transmit power than a per-cell power control solution; 2) increases network throughput by up to 50% in the WLAN; 3) increases the throughput of asymmetric links by 300%; and 4) deduct the power usage of mobile nodes transmit by 97% for of mobile nodes.

Merits of the existing techniques are follows:

**Packet Scheduling Algorithms**

Scheduling algorithms determine which packet is served next among the packets in the given queue model. Here scheduler is situated between the routing specialist and the MAC layer. Every mobile node utilizes a similar scheduling algorithm for routing the data packets. In this model, it consider the conventional scheduling (priority scheduling) usually used in mobile ad hoc networks[6]. In buffer management, drop tail policy is utilized with no-priority scheduling and it works when buffer is empty otherwise drops the incoming packets. For the scheduling algorithms that give high priority to control packets, we use different drop policies for data packets and control packets when the buffer is full. In given queue, if incoming packet is a control packet, we drop the last en-queued data packet, if any exists in the buffer, to make space for the control packet. If all queued packets are control packets, we drop the incoming control packet.

Demerits of the existing models are as follows:

- The carrier sense multiple access with collision avoidance (CSMA/CA) relies on the fair carrier sense.
- The carrier sense mechanism is used to detect whether there are any other devices in transmitting.
- The sensed node with short transmission range results in starvation problem.

### III. PROPOSED SYSTEM

#### A. Overview and Important Properties of the Protocol

The DSR protocol [7] is consist of mainly two functionalities that used in the ad hoc network in order to discover and maintain the source routes: In Route Discovery mechanism of the DSR protocol a node S wishing to send a packet to a destination node D will obtain a source route to D. Only When S attempts to send a packet to D the Route Discovery Protocol will be used and the route to D will not be pre defined. In the Route Maintenance mechanism a node S will be able to detect, when a source route to D is used, and the network topology will be changed in such a way that its route to D will be no longer available because a link along the route no longer works. S can try to use any other route to D, or Route Discovery Mechanism can be used to find a new route, when the Route Maintenance Mechanism indicated that the source route is broken. when S is sending packets to D is the only instance when the Route Maintenance Mechanism is actually used. Both Route Discovery and Route Maintenance are operated based on demand. Actually DSR protocol is different from other protocols in the facts such as, DSR does not need periodic packets in any form. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbor detection packets, and the functions do not rely on the methods form existing protocols. This entirely on-demand behavior and lack of periodic activity allows the number of overhead packets caused by DSR to balance them to zero, if every node is roughly stationary in respect of each other and all routes needed for current communication have already been discovered. When nodes start roaming the network the pattern of communication changes by the routing packet overhead of DSR automatically scales to only that needed to track the routes currently in use[10]. In response to a single Route Discovery (as well as through routing information from other packets overheard), a node may learn and cache multiple routes to any destination. This allows the reaction to routing changes to be much more rapid, since a node with multiple routes to a destination can try another cached route if the one it has been using should fail. This caching of multiple routes also avoids the
overhead of needing to perform a new Route Discovery each time a route in use breaks. Unidirectional links and asymmetric routes are easily supported by the Route Discovery and Route Maintenance mechanism in DSR. In wireless networks, communication between two nodes won\'t work in the usual manner in a symmetrical way. This is because of patterns generation or source interference. DSR admits asymmetrical communications when needed, thus improves the performance and communication. DSR also supports internetworking between different types of wireless networks [8], allowing a source route to be composed of hops over a combination of any types of networks. For example, in ad-hoc networks, few nodes works with short-range radios, while other nodes with both short-range and long-range radios; the combination of these nodes together can be considered by DSR as a single ad-hoc network. In addition, the routing performed in DSR has been combined into conventional routing method, where a gateway node connected to the Internet also involved in the ad-hoc network routing protocols; and has been integrated into Mobile IP routing, where such a gateway node also serves the role of a Mobile IP.

**B. System Model**

![Diagram of Network Flooding of RREQ and Propagation of RREP Message]

Widespread analysis and research are being conducted in reduction of malnourishment in mesh networks as it is a main issue in wireless mesh networks. As per the literature in the author introduced an algorithm called Fair Binary Exponential Backoff algorithm, is the expansion of Binary Exponential Backoff algorithm (BEB). Broadly used binary exponential backoff algorithm used to adjusts the contention window size by approximating the network traffic in communication channel in every node level in effect by counting consecutive collisions concerning the packet. The FBEB algorithms affirm that the successful transmitted packet in the node will not reset its contention window for the next transmission; it has to wait for a time T. resetting the current node will allow others to use the channel. The time T depends on the previous contention in the network. But this algorithm also affirm that packet collision arise the contention window in the increased rate. Again the process begin, if the contention window overflows it is reset and the packets would be left out. If the contention window is doubled it becomes problem to other nodes which suffer from starvation. So to overcome these problems here proposed a new algorithm called Starvation Mitigation Algorithm (SMA) in which the gateway acts as an intermediate node to take decisions and broadcasts a message about starvation by channel access continuously without giving a chance to remaining nodes. Then by receiving this message remaining.

The fundamental explanation behind starvation is that, the nodes which are near the entryway won\'t allow to different nodes for getting to the channel. So the stream gets starved and the data transfer capacity is not productively used by the system. So to stay away from this issue we present a Starvation Mitigation Algorithm (SMA) by which we can give productive data transfer capacity use by every one of the nodes in a network and give decency in a network[6].

Merits of the proposed system as follows:

- Starvation is reduced in the networks.
• Mesh nodes that have successfully transmitted data packets should not be permitted to transmit more data packets.
• Degree of starvation is reduced.
• The types of traffic to analyze the level of starvation such that the non-necessary adjustments are reduced.

C. System methodologies

- Basic DSR Route Discovery
- Basic DSR Route Maintenance
- Additional Route Discovery Features
- Additional Route Maintenance Features
- Support for Heterogeneous Networks and Mobile IP
- Multicast Routing with DSR

**Basic DSR Route Discovery**

When a node initiates a new packet intended to some other node, it places in the header of the packet a source route giving the sequence of hops that the packet should follow on its way to end node. Normally, the source node will attain a appropriate route by searching its Route Cache of routes from last learned [7], but if no route is found in its cache, it will initiate the Route Discovery protocol to find a novel route to end node in dynamic way. In this case, we call S the initiator and the end of the Route Discovery. Each ROUTE REQUEST message identifies the source and destination node of the Route Discovery, and also contains a unique request identifier, resolved by the initiator of the REQUEST. Each ROUTE REQUEST also contains a record listing the address of each node in the path is particular copy of the ROUTE REQUEST message has been forwarded. This route record is initialized to an empty list by the initiator of the Route Discovery. When a node receives a ROUTE REQUEST, if it is the end of the Route Discovery, it returns a ROUTE REPLY message to the initiator of the Route Discovery, giving a copy of the gather route details from the ROUTE REQUEST; when the initiator receives this ROUTE REPLY, it caches this route in its Route Cache for use in transferring succeeding packets to the end node. Or else, if the node getting the ROUTE REQUEST has recently seen another ROUTE REQUEST message from this initiator bearing this same request identifier, otherwise it locates its own address is previously programmed in the route record in the ROUTE REQUEST message, it discards the REQUEST. Otherwise, this node appends its own address to the route details recorded in the ROUTE REQUEST message and transmits it by conveying it as a local broadcast packet (with the same request id). This limitation on the maximum rate of Route Detecting for the similar end node is same to the method mandatory by network nodes to limit the rate at which ARP REQUESTs are sent for any single target IP address.

**Basic DSR Route Maintenance**

When initiate or forward a packet using a source route, each node transmitting the packet is responsible for confirming that the packet has been received by the next hop down the source path, the packet is retransmitted until this confirmation of receipt is received.

**Additional Route Discovery Features**

Caching Overheard Routing Information of node forwarding or overhearing a packet add the routing information from that packet to its own Route Cache. In particular, the source route used in a packet, the buildup route details in a ROUTE REQUEST, or the route returned in a ROUTE REPLY may all be cached by any node. Routing information from any of these packets expected have been cached, when the packet was concentrated on to this node, perform a broadcast (or multicast) MAC address[8], or received while the node’s network interface is in promiscuous mode. One demerit, storing of such overheard routing information is the possible presence of uni-directional links in the
ad hoc network. Similar considerations apply to the routing details may be obtained from forwarded or otherwise overheard ROUTE REQUEST or ROUTE REPLY packets.

**Additional Route Maintenance Features**

**Packet Salvaging**

When receiving a ROUTE ERROR message while Route Maintenance, the source node may recover the data packet that creates the ROUTE ERROR. It does not discarding it. To attempt to salvage a packet, the node pass a ROUTE ERROR finds its Route Cache for a route from itself to the destination of the packet causing the ERROR. If such a route is found, the node may salvage the packet after recurring the ROUTE ERROR in the place of original source route on the packet with the route from its Route Cache. The node then forwards the packet to the next node indicated along this source route. Current salvaging mechanism allows backtracking but prevents a packet from being salvaged more than once.

**Automatic Route Shortening**

Source routes by itself condensed if many hops in between the path have been needed. This mechanism of automatically shortening routes in use is somewhat similar to the use of passive knowledgements. In particular, if a node is able to eavesdrop a data packet carrying a source route, then the node inspects the idle portion of that initial route. If source node is not the future the next hop for the packet but is named in the later unused portion of the packet’s source route, then it can conclude that the middle nodes itself in the source route are no longer needed in the route.

**Support for Mobile IP**

In configuring and deploying an ad hoc network, in many cases, all nodes will be equipped with the same type of wireless network interfaces, allowing simple routing between nodes over arbitrary sequences of network hops. An easy pattern has been equipped as a subset of the nodes with a second network interface consisting of a longer-range wireless network interface. Say in a military setup, a gang of soldiers might all use short-range radios to communicate among themselves, while relaying through truck-mounted higher power radios to communicate with other groups.

This category of network pattern is the ad-hoc networking same as of wireless overlay networks [12]. Due to the high degree of locality likely to be present among openly assisting nodes communicating with each other, such thing would allow high speed communication among such cooperating nodes, while at the same time allowing communication with other nodes availed without large numbers of hops. The longer-range radios might also allow gaps between different groups of nodes to be spanned, reducing the probability of network partition.

**Use of Interface Indices**

DSR supports automatic, seamless routing in these and other heterogeneous configurations, through its logical addressing model [7]. Using conventional IP addressing, each ad-hoc network node would construct various IP addresses for each of its possibly many network interfaces, each node with DSR chooses one of the home addresses to use for all communication while in the ad hoc network. This use of a single IP address per node made DSR to handle all the nodes in network as single domain. To then distinguish between the different network interfaces on a node, each node assigns a locally unique interface index to each of its own network interfaces without any interruption. The interface index for any network interface on a node is an opaque value given by the node itself. The specified value chosen must be unique among the network interfaces on that each node with no importance need not be coordinated with any other nodes in choosing their own interface indices. On many operating systems, each network interface is identified by a unique value and can be used for this purpose; for example, the if index field in the if net structure for a network interface in BSD
Unix-based networking stacks [6] can be used directly by a node for the interface index for that network interface.

IV. CONCLUSION

AODV routing protocol uses Weight hop based packet scheduling in this model. The impact of various scheduling algorithms for AODV and modified AODV was assessed. The routing protocol and portability demonstrate the packets in queue composition. As a result of data traffic there is a network congestion delay during low mobility. Where as in at High mobility, its influenced by route changes in replication results. Preparing algorithms that give higher weightage to data packets with littler quantities of hops or shorter geographic separations to their goals diminish normal postponement fundamentally with no extra control parcel trade. This is used for customization AODV. Result demonstrates impressively littler postponement than the other planning Algorithms. The lessening in the normal postpone diminishes as the portability of nodes.

REFERENCES