Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks

MODULE 1:

wireless topology of creation of simple packet transmission between nodes with default node configurations.

Flow of Implementation:

TCL Script, Default configurations of wireless,AODV protocol,NAM window.

EXISTING MECHANISM (PAPERS EXISTING METHOD)

MODULE 2:

wireless sensor network topology of creation of more number of nodes [50 nodes] with default node configurations and packet transmission will be done based on NORMAL SCHEME and QOS performance metrics like end to end delay, energy spent, packet delivery ratio, throughput, attack detection rate values are taken and graphs will be plotted in xgraph.

Flow of Implementation:

TCL Script, Default configurations of wireless,AODV protocol,NAM window,awk file execution,graph plot.

MODULE 3:

wireless sensor network topology of creation of more number of nodes [50 nodes] with default node configurations and packet transmission will be done based on NORMAL SCHEME and selective forward attack has been introduced in the network to check the network performance where as QOS performance metrics like end to end delay, energy spent,packet delivery ratio, throughput,collision rate values are taken and graphs will be plotted in xgraph. Selective Forward Attack will minimize the network life time by packet drops and the same can be seen in NAM so performance of the network gets degraded.

Flow of Implementation:

TCL Script, Default configurations of wireless, procedure written for attack,AODV protocol, NAM window, awk file execution, graph plot.

PROPOSED MECHANISM (PAPERS PROPOSED METHOD)

MODULE 4:

wireless sensor network topology of creation of more number of nodes [50 nodes] with default node configurations and packet transmission will be done based on CRS-A: THE CHANNEL-AWARE REPUTATION SYSTEM WITH ADAPTIVE DETECTION THRESHOLD CRSA PROTOCOL and selective forward attack has been introduced in the network to check the network performance where as QOS performance metrics like end to end delay, energy spent, packet delivery ratio, throughput, attack detection ratio values are taken and graphs will be plotted in xgraph. Selective Forward Attack will be detected by the CRSA protocol and network life time, performance will gets increased

Flow of Implementation:

TCL Script, Default configurations of wireless, procedure written for attack, procedure for CRSA PROTOCOL ,PROPOSED protocol,NAM window,awk file execution,graph plot.

MODULE 5:

Comparison between the all the above techniques with single trace file and graphs execution is done with xgraph.

Flow of Implementation:

User generated trace files,graph plot.

NOTE:

SOFTWARES USED : REDHAT LINUX 9

Front End : TCL

Back End : C++

This PROPOSED TECHNIQUE is only for detection of attacks so to prevent attacks a new model should be developed so enhancement (New work with the paper) has not given in the module break up. If the student has any idea on the same please contact else we will suggest you once we completed the paper work.