Secure Data Collection in Wireless Sensor

Networks Using Randomized Dispersive Routes

AIM:

In this Project, we study data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. We argue that classic multipath routing approaches are vulnerable to such attacks, mainly due to their deterministic nature

PURPOSE:

In this Project, we propose a randomized multipath routing algorithm that can overcome the above problems. In this algorithm, multiple paths are computed in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination

DESCRIPTION:

Compromised node and denial of service are two key attacks in wireless sensor networks (WSNs). In this paper, we study data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. We argue that classic multipath routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once the adversary acquires the routing algorithm, it can compute the same routes known to the source, hence, making all information sent over these routes vulnerable to its attacks. In this paper, we develop mechanisms that generate randomized multipath routes. Under our designs, the routes taken by the “shares” of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes. We analytically investigate the security and energy performance of the proposed schemes. We also formulate an optimization problem to minimize the end-to-end energy consumption under given security constraints. Extensive simulations are conducted to verify the validity of our mechanisms

Existing System:

With the existing system while using to the Compromised Node [CN] transferring the data there is no security constraints are added. Even though you are transferring the data .The whole application will be struck.

Proposed System:

In that proposed system replaced the disadvantage in Existing System. Means the ES (Existing System) while using the DOS (Denial of Services) Node to transferring the data when hacker will be hack the particular router. At that movement DOS node to be selected to a multipath routing .so there is no data losing.

Module Description:

In this Project we have 4 modules there are:

* Server
* Client
* Router
* Hacker

**Server:**

When client will be ask the request to server .at that time server will be give the response and receiving that data’s.

**Client:**

Send the data to server while server is response that client

**Router:**

It is intermediator between the Server and Client. When hacker will be hack the router .the router will be give that information to the client when Router working DOS Node. Otherwise is not given.

**Hacker:**

In this module hack to the client and server information or data’s.

**SYSTEM REQUIREMENTS**

Hardware Requirements:

Processor : Pentium III / IV or Above

Hard Disk : 40 GB

Ram : 256 MB

Monitor : 15VGA Color

Software Requirements:

Operating System : Windows XP professional

IDE : Microsoft Visual Studio .Net 2005

Language : Visual C#.Net

Back End : SQL Server 2000

Conclusion:

Our analysis and simulation results have shown the effectiveness of the randomized dispersive routing in combating CN and DOS attacks. Appropriately setting the secret sharing and propagation parameters, the packet interception probability can be easily reduced by the proposed algorithms to as low as 10\_3, which is at least one order of magnitude smaller than approaches that use deterministic node-disjoint multipath routing. At the same time, we have also verified that this improved security performance comes at a reasonable cost of energy. Specifically, the energy consumption of the proposed randomized multipath routing algorithms is only one to two times higher than that of their deterministic counterparts. The proposed algorithms can be applied to selective packets in WSNs to provide additional security levels against adversaries attempting to acquire these packets. By adjusting the random propagation and secret sharing parameters (N and M), different security levels can be provided By our algorithms at different energy costs. Considering that the percentage of packets in a WSN that require a high security level is small, we believe that the selective use of the proposed algorithms does not significantly impact the energy efficiency of the entire system