**Providing End-to-End Secure Communications**

**in Wireless Sensor Networks**

Abstract:

Providing desirable data security, that is, confidentiality, authenticity, and availability, in wireless sensor networks (WSNs) is challenging, as a WSN usually consists of a large number of resource constraint sensor nodes that are generally deployed in unattended/hostile environments and, hence, are exposed to many types of severe insider attacks due to node compromise. Existing security designs mostly provide a hop-by-hop security paradigm and thus are vulnerable to such attacks. Furthermore, existing security designs are also vulnerable to many types of denial of service (DoS) attacks, such as report disruption attacks and selective forwarding attacks and thus put data availability at stake. In this paper, we seek to overcome these vulnerabilities for large-scale static WSNs. We come up with a location-aware end-to-end security framework in which secret keys are bound to geographic locations and each node stores a few keys based on its own location. This location-aware property effectively limits the impact of compromised nodes only to their vicinity without affecting end-to-end data security. The proposed multifunctional key management framework assures both node-to-sink and node-to-node authentication along the report forwarding routes. Moreover, the proposed data delivery approach guarantees efficient en-route bogus data filtering and is highly robust against DoS attacks. The evaluation demonstrates that the proposed design is highly resilient against an increasing number of compromised nodes and effective in energy savings.

Existing System:

**In many Wireless Sensor Networks (WSNs), providing end to end secure communications between sensors and the sink is important for secure network management. While there have been many works devoted to hop by hop secure communications, the issue of end to end secure communications**

**Is largely ignored**

**Proposed System:**

**In this paper, we design an end to end secure communication protocol in randomly deployed WSNs.**

**Specifically, our protocol is based on a methodology called differentiated key pre-distribution. The core idea is to distribute different number of keys to different sensors to enhance the**

**resilience of certain links. This feature is leveraged during routing, where nodes route through those links with higher resilience. Using rigorous theoretical analysis, we derive an expression for the quality of end to end secure communications, and use it to determine optimum protocol parameters. Extensive performance evaluation illustrates that our solutions can provide highly secure communications between sensor nodes and the sink in randomly deployed WSNs. We also provide detailed discussion on a potential attack (i.e. biased node capturing attack) to our**

**solutions, and propose several countermeasures to this attack.** in WSNs, we need to use hop by hop based encryption/decryption inproviding end to end secure communications.

Modules:

**Client**

**Server**

**router(Sensor)**

**HARDWARE AND SOFTWARE REQUIREMENTS**

**Software Requirements:**

Language : C#.NET

Technologies : Microsoft.NET Framework,

 ADO.NET

IDE : Visual Studio 2008

Backend : SQL Server 2005

Operating System : Microsoft Windows XP SP2 or Later Version

**Hardware Requirements:**

Processor : Intel Pentium or more

RAM : 512 MB (*Minimum*)

 Hard Disk : 40 GB