ABSTRACT

Wireless Sensor Network (WSN) is used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSN. However, WSN suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. Hence to providing security for sensor network is very important. Utilizing sensor nodes make unfeasible to use traditional energy efficient routing techniques such as LEACH, DSR, Flooding, directed diffusion and key management techniques such as public key cryptography for security service of sensor network. The security issues such as data integrity, confidentiality, and freshness in data aggregation become crucial when the WSN is deployed in a remote or hostile environment where sensors are prone to node failures and compromises. This work focused on secure routing, key management, secure data aggregation and data collection in WSN. There is currently a research potential in securing data aggregation in the WSN.

This research work investigates three security problems existing in the above counter-attack approach. First, this approach is no longer valid if the adversary can selectively compromise or jam nodes. This is because the route computation in the above multi-path routing algorithms is deterministic in the sense that for a given topology and given source and destination nodes, the same set of routes is always computed by the routing algorithm. As a result, once the routing algorithm becomes known to the adversary, it can compute the set of routes for any given source and destination. Then the adversary can pinpoint to one particular node in each route and compromise (or jam) these nodes. Such an attack can intercept all shares of the information, rendering the above counter-attack approach is
ineffective. Second, actually very few node-disjoint routes can be found when the node density is moderate and the source and destination nodes are several hops apart. Last, because the set of routes is computed under certain constraints, the routes may not be spatially dispersive enough to circumvent a moderate-size black hole. In reality, a stronger attack could be formed, whereby the adversary selectively compromises a large number of sensors that are several hops away from the sink to form clusters of black holes around the sink.

The contribution of this thesis is mainly focused on secure data collection and aggregation. The Sensor network is a collection of sensor nodes which cooperatively send sensed data to sink node. After sensing, each sensor has to deploy dense data to the base station, by which WSN can successfully operate in the presence of component failures or densely compromise node attack. In order to overcome these, it can be solved by using Cartesian product sets, Inductive Reasoning Implementation and Translating Method. Therefore this research was delineated with development of algorithms includes New Sequence Key (NSKey) Algorithm, avoid Densely Traffic Collusion Attack. Another Path File List (PFlist) Algorithm access the sink node to determine and compute the aggregate (SRA Value) if any wrong contribution occured. Further this work admitted to design the energy efficient secure data Routing protocol for Data collection and Aggregation in Wireless Sensor Network. In brief, the whole work was contented with GBSD security protocol, provided positive features of symmetric key cryptography and it created the secrete key, which reduced the malicious node and keep data fresh. Also it generated a large odd even number and it fixed the period for symmetric key to keep data integrity and to avoid the replay attack. Usually, the well designed security scheme is essential for the further development and the success of wireless sensor network. However, this work postulated the security schema consists of two security level. The first level was generated the log files within a specified path maintance for analyze the data value. The second level was Key distribution method for devising a key management scheme solution for Match key rekeying also exploits the idea of key solution using a hash chain in order to achieve key secrecy. The central idea is to incorporate statistical properties extracted from the sensory data
into the belief model. Hence, this work acquired method for data collection to prolong the network lifetime and branch based Fast relay running branch protocol (FRRBP) in mobile sink sensor networks, the LRCS Protocol can achieve secure aggregation for other aggregation functions including sum, histograms of data distribution or range queries. Consecutively, it also analyzed the compromised node attack which is one of the network layer attacks. This kind of attacker launches attacks by forming a tunnel between two or more malicious nodes and drops all the packets. The LCRS Path File List (PT) algorithm used to detect and prevent the wormhole attack using per hop distance between two nodes. Our proposed algorithm implementation depends on DSR protocol.

Finally NS2, Java, Lab Modeler, WiseNet simulation is used to develop and test algorithm which are likely to arise during the research. The simulation parameters like throughput, overhead and the average delay of the proposed algorithm are compared with that of existing wormhole prevention techniques. From the simulation and analysis of results, it is clear that our proposed algorithm is more effective in preventing the wormhole attack with greater throughput and less average delay. The performance analysis addresses that PFL algorithm has reduced overhead and delay. These results, along with advantage that no additional requirement of hardware makes the proposed system more suitable for resource constrained wireless network application. The simulation results indicate that our aggregation function can be achieve an energy saving under various attack patterns with different ratios of compromised nodes and reason about the uncertainty in the aggregation results. Future research in Routing, cross-layer design can focus on collaboration between all the layers to achieve higher energy saving, network performance and extend network lifetime. Its resolution requires us to extend our mechanisms to handle multiple collaborating black holes, which have to be studied and developed in my future work.