5.1 Introduction

Chapter works on the third non functional IoT architecture feature as security. The Internet of thing is a network of physical things, which can be stationary or movable. An Ad hoc network can be part of IoT. Mobile Ad-hoc networks (MANET) [173] can be dynamic and can be prone to a number of security problems. Legacy Internet systems and new Internet of Things, causes many security problems and lead to a big security framework. A mobile node becomes a foreign node for the fixed network. This foreign node can be really helpful in forwarding packets or maybe pretending to do so. The intentions of the foreign nodes are normally not clear and indirectly may make unsecure communication. If such a node exists, the network should provide basic and important security services such as availability, integrity, confidentiality, authenticity, and non repudiation. For this security services encryption, hashing, digital certificates, and digital signatures, etc can be applied as some of the mechanisms. Malicious nodes can cause isolation of nodes, or it can make starve node from connecting to its peer node, or even it may provide wrong or useless validations. Nodes, which pretend to co-operate and create problems in providing the correct destination path by giving wrong validations are called as malicious nodes in the grey hole attacks. Precautionary steps need to be taken against such malicious node attacks.

Few of these attacks are black hole, grey hole, and their co-operative attacks, which absorb all or some information in the form of packets. This leads to data loss. There are lots of detection and prevention mechanisms to stop such attacks of black and grey holes. All types of Black, Grey, and their co-operative hole attacks are still topics of research. A proposed algorithm is an extension of algorithm [174]. An algorithm reduces the number of tests conducted on all nodes engaged in transmission (some algorithms keep on checking the acknowledgements of received packets across all paths every time), and contributes in saving the battery life of constrained devices.

Section one outlines the chapter flow, and explains the basic concepts of security, grey, black, and co-operative grey holes and their behaviours. Chapter proposes a solution for the detection of grey and their co-operative attacks by using the Ad hoc On-Demand Distance Vector (AODV) protocol as a base protocol. AODV is considered because of its scalability, easy implementation, and efficient resource utilization. Section two, connects the legacy security framework with IoT framework. Framework tries to acquaint readers with all possible tasks required to be implemented for any type of security attack. Section three puts