1.

Record Nr.	TD17055985
Autore	Khan, Sarmad Ullah
Titolo	Key Management in Wireless Sensor Networks, IP-Based Sensor Networks, Content Centric Networks [Tesi di dottorato]
Editore	Politecnico di Torino, 2013
Lingua di pubblicazione	Inglese
Formato	Tesi di dottorato
Livello bibliografico	Monografia
Note	In relazione con http://porto.polito.it/2506342/
Sommario	Cryptographic keys and their management in network communication is considered the main building block of security over which other security primitives are based. These cryptographic keys ensure the privacy, authentication, integrity and non-repudiation of messages. However, the use of these cryptographic keys and their management in dealing with the resource constrained devices (i.e. Sensor nodes) is a challenging task. A number of key management schemes have been introduced by researchers all over the world for such resource constrained networks. For example, light weight PKI and elliptic curve cryptography schemes are computationally expensive for these resource constrained devices. So far the symmetric key approach is considered best for these constrained networks and different variants of it been developed for these networks (i.e. probabilistic key distribution approach). The probabilistic key distribution approach consumes less memory than the standard symmetric key approach but it suffers from the connectivity issues (i.e. the connectivity depends on the common shared keys between the nodes). Most of those schemes were proposed by considering static sensor networks (e.g. Industrial process monitoring, Environmental monitoring, movement detection in military applications, forests etc.). However, the use of these existing key management schemes for mobile wireless sensor networks applications introduces more challenges in terms of

network connectivity, energy consumption, memory cost, communication overhead and protection of key materials against some well known attacks. Keeping these challenges in mind, previous research has proposed some key management schemes considering the mobility scenarios in ad hoc networks and wireless sensor networks (e.g. vehicular networks, health monitoring systems).However these schemes consume more resource because of a much higher communication packet exchange during the handover phase for the authentication of joining and leaving nodes than the static networks where there is no extra communication for the handover and authentication. The motivation of this research work is to investigate and propose new algorithms not only to improve the efficiency of these existing authentication and key management schemes in terms of connectivity, memory and security by considering the mobility scenario in wireless sensor networks, but also to develop new algorithms that suit these constrained networks than the existing schemes. First, we choose the existing key pool approach for authentication and key management and improve its network connectivity and resilience against some well known attacks (e.g. node capturing attacks) while reduce the memory cost by storing those key pools in each sensor node. In the proposed solution, we have divided the main key pool into two virtual mutually exclusive key pools. This division and constructing a key from two chosen keys, one from each key pool, helps to reduce the memory cost of each node by assigning fewer keys for the same level of network connectivity as the existing key pool frameworks. Although, the proposed key pool approach increases the network resilience against node compromission attacks because of the smaller number of keys assigned to each node, however it does not completely nullify the effect of the attacks. Hence we proposed an online mutual authentication and key establishment and management scheme for sensor networks that provides almost 100\% network connectivity and also nullifies the effect of node compromission attacks. In the proposed online key generation approach, the secret key is dependent on both communicating parties. Once the two communicating parties authenticate each other, they would successfully establish a secret communication key, otherwise they stop communication and inform the network manager about the intruder detection and activity. The last part of the thesis considers the integration of two different technologies (i.e. wireless sensor networks and IP networks). This is a very interesting and demanding research area because of its numerous applications, such as smart energy, smart city etc.. However the security requirements of these two kind of networks (resource constrained and resourceful) make key management a challenging task. Hence we use an online key generation approach using elliptic curve cryptography which gives the same security level as the standard PKI approach used in IP networks with smaller key length and is suited for the sensor network packet size limitations. It also uses a less computationally expensive approach than PKI and hence makes ECC suitable to be adopted in wireless sensor networks. In the key management scheme for IP based sensor networks, we generate the public private key pair based on ECC for each individual sensor node. However the public key is not only dependent on the node's parameter but also the parameters of the network to which it belongs. This increases the security of the proposed solution and avoids intruders pretending to be authentic members of the network(s) by spreading their own public keys. In the last part of the thesis we consider Content Centric

Networking (CCN) which is a new routing architecture for the internet of the future. Building on the observation that today's communications are more oriented towards content retrieval (web, P2P, etc.) than point-to-point communications (VoIP, IM, etc.), CCN proposes a radical revision of the Internet architecture switching from named hosts (TCP/IP protocols) to named data to best match its current usage. In a nutshell, content is addressable, routable, self-sufficient and authenticated, while locations no longer matter. Data is seen and identified directly by a routable name instead of a location (the address of the server). Consequently, data is directly requested at the network level not from its holder, hence there is no need for the DNS). To improve content diffusion, CCN relies on data distribution and duplication, because storage is cheaper than bandwidth: every content - particularly popular one - can be replicated and stored on any CCN node, even untrustworthy. People looking for particular content can securely retrieve it in a P2P-way from the best locations available. So far, there has been little investigation of the security of CCNs and there is no specific key management scheme for that. We propose an authentication and key establishment scheme for CCNs in which the contents are authenticated by the content generating node, using pre-distributed shares of encryption keys. The content requesting node can get those shares from any node in the network, even from malicious and intruder ones, in accordance with a key concept of CCNs. In our work we also provide means to protect the distributed shares from modification by these malicious/intruder nodes. The proposed scheme is again an online key generation approach but including a relation between the content and its encryption key. This dependency prevents the attackers from modifying the packet or the key shares

Localizzazioni e accesso	http://memoria.depositolegale.it/*/http://porto.polito.it/2506342/1/Sarmad_Ullah_Khan_PhD_Thesis.pdf