Survey on Security Mechanisms for Routing Over 6LoWPAN

Alagumeenaakshi Muthiah*[1], Dr. S. Palaniswami[2]

**1 Dept. of ECE, Kumaraguru College of Technology, Coimbatore, India*
2 Principal, Government College of Technology, Bodinayakanur, India

Abstract: **In a wireless sensor network (WSN) environment, a sensor node is extremely constrained in terms of hardware due to factors such as maximizing lifetime and minimizing physical size and overall cost. The different security challenges that may arise in integrating WSN to Internet of Things (IoT) are to be specially focused. High attention, however, is given to the routing protocols since they might differ depending on the application, path selection, network architecture and protocol operation. This paper surveys recent routing protocols for sensor networks and presents a classification for the various approaches pursued based upon the application and the available hardware motes. Enormous survey towards threats, vulnerabilities and various routing protocols has been done and a holistic overview of security requirements and issues for using IETF's RPL routing protocol over 6LoWPAN is given. Along the way, effort has been made towards the classification and analysis of secure routing schemes in literature and the advantages and disadvantages in each category has been discussed. The open research issues in establishing secure routing over 6LoWPAN are envisaged.**

Keywords: Routing protocols, WSN, Secure RPL, IPv6, 6LoWPAN.

I. INTRODUCTION

Advantages in communication technology allow us to build the networks where large numbers of low-power and inexpensive sensor devices are integrated in the physical environment and operating together over a wireless media. The sensor nodes have special functions to sense and collect information about the environment under monitoring: temperature, humidity, illumination, noise and so on [1]. Application domains of Wireless Sensor networks are widely developing in various areas. In the near future, everyday objects that surround us will become a part of Internet that can generate and consume information. Security in WSNs is a challenging task due to inherent limitations of sensors.

All the functionality of the sensor networks is provided thanks to the individual capabilities of sensor motes. Each sensor node with less computational capability has several built-in sensors and can communicate wirelessly. Therefore, they have the capacity to collect and process the raw information about their surroundings and communicate with neighbors. Nodes are also small in size, and can unobtrusively provide the physical information of any entity. Moreover, nodes are usually battery powered enabling them to act independently and operate autonomously if required. Base station is a powerful and capable device that serves as an interface between the sensor nodes and the user. An efficiently designed sensor network is built with long term goals in mind. Often a limited opportunity exists to deploy any sort of network and the initial setup must be maintained throughout measurements. For example, a network deployed on the seafloor by a research vessel cannot easily modified, yet may be expected to collect data from environments over-saturating the test bed with sensors. A WSN must be a self organizing structure, so as the topology of the network changes, connections remain wherever possible. As motes begin to fail, others are expected to step up and fill in. Similarly, some devices may be programmed to wake up late in the life of a network in order to extend its life. An ideal implementation might take into account of battery power and expected lifetime of each node to maximize dependability.

A set of new manifold options is arriving to the WSN based on IEEE 802.15.4 LLNs (Low power and Lossy Networks) with the connectivity to the IP world, with the solutions defined by the Internet Engineering Task Force(IETF), 6LoWPAN [2]. Similar to WSN, 6LoWPAN's sensor nodes are also resource constrained with small data rate, low bandwidth and low transmit power. The major issues among them are power consumption and network lifetime extension [4]. Secure routing is one of the key challenges for 6LoWPAN WSN and the challenge becomes more difficult when the network size is growing and the hardware resources are restricted. Also this standard is considered as a suitable candidate to introduce the concept of "Internet of Things" (IoT) to the real world.

These challenges necessitate energy awareness at all layers of networking protocol stack. Usually, the physical and link layer issues are very common to any sensor application, therefore concentrating the research on system-level power awareness such as dynamic voltage scaling, radio communication hardware, low duty cycle issues, system partitioning, energy-aware MAC protocols [20]. At the network layer, the main aim is to find ways for energy-efficient route setup and reliable relaying of data from the sensor nodes to the sink so that the lifetime of the network is maximized. In this scenario, any protocol, architecture or application which is not developed with security in mind is hardly useful. In this paper, we present a survey of the "state-of-the-art" security issues and algorithms that a designer must have in mind while working with current

scenario of IoT and WSN. Section 2 presents related work and the background leading to the solution described in section 3. Further development possibilities are outlined in section 4 and conclusion in section 5.

The contribution of this paper is arranged as follows

1. First the limitations of Wireless Sensor Networks are discussed
2. The threat models and the attacks on the Sensor Networks are discussed.
3. Applications of WSN.
4. Security Objectives and requirements are listed.
5. The current Routing Protocols are classified and analyzed with advantages and disadvantages of each of them.
6. Focus on the research issue.

1.1 Limitations In Sensor Networks

The following section list the inherent limitations in the sensor networks which make the design of the security procedures complicated. Routing in sensor networks is very challenging due to these several characteristics

1. Sensor nodes are tightly constrained in terms of power, on-board energy, storage and processing capacity and thus require careful resource management.
2. Lack of infrastructure leads to insecure wireless communication.
3. Deployment nature in public and hostile environments makes them highly vulnerable to capture and vandalism. Physically security of sensor nodes with tamper proof material results in increased cost of a node.
4. Classical IP-based protocols are not suitable due to lack of global addressing scheme.
5. Compared to communication networks, most applications demand MP2P traffic from multiple regions (sources) to a base station (sink).
6. Optmization of energy and bandwidth utilization has to be exploited by routing protocols to reduce redundancy of data in the vicinity of sink node.
7. Sensor nodes can easily be compromised.
8. Heterogeneous nature of the sensor nodes used for deployment is an additional limitation.
9. The topology of a WSN changes very frequently due to the failures, joining or mobility of nodes.
10. Dense deployment of sensor nodes in several orders of magnitude higher than that in an ad-hoc network.

Due to such differences, many new algorithms have been proposed for the problem of routing data in sensor networks. The mechanisms of routing are classified considering the characteristics of sensor nodes regarding path selection, network architecture and protocol operation apart from its application.

The cryptographic techniques devised for the traditional wired networks are not feasible to Wireless Sensor Networks. Encryption leads to extra processing, memory and battery power which are the prime resources for the sensors' longevity. The security mechanisms could also increase delay, jitter and packet loss in wireless sensor networks [12]. Due to minimal or no human interaction possibility for the sensors, time to time modification of keys for encryption is also an important issue. The methods of managing, revoking and assigning keys to a new sensor that is added to the network or renewal of keys for ensuring robust security must be taken under consideration. Adoption of pre-loaded keys or embedded keys could not be an efficient solution.

1.2 Applications Of Wireless Sensor Networks

There are many areas of application that can take advantage of all these benefits. The applications can be classified into the following categories:

1. Monitoring space. The sensor network simply monitors the physical features of a certain environment. This category includes applications such as environmental and habitat monitoring, precision agriculture, indoor climate control, surveillance, treaty verification, and intelligent alarms.

2. Monitoring things. The sensor network controls the status of a physical entity. This category includes applications such as structural monitoring, eco-physiology, condition-based equipment maintenance, medical diagnostics, and urban terrain mapping.

3. Monitoring interactions. The sensor network monitors the interactions of things (both inanimate and animate) with each other and the encompassing space. This category includes applications such as wildlife habitats, disaster management, critical (information) infrastructure systems, emergency response, asset tracking, healthcare, and manufacturing process flow.

While all the application areas presented in the previous classification are mere ideas of where WSN could be applied, the research community has already proven the usefulness of WSN in real-world settings. [28]

1.3 Threat Models

Any WSN environment is prone to threats and attacks from the adversaries. The major classification of the threat models due to adversary nodes can be modelled as listed below:

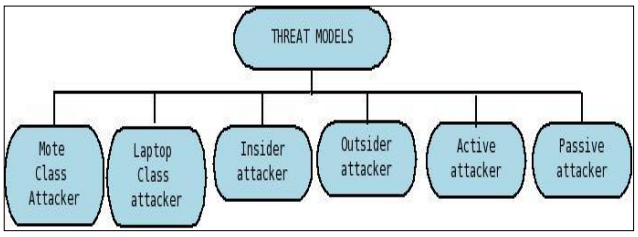


Fig. 1. Classification of Threat Models

Mote-class attacker vs. Laptop-class attacker: A mote-class attacker has similar capabilities as other motes and hence can access to only a few motes in the network whereas a laptop-class attacker has access to devices with more computational resources resulting in serious attacks.

*Inside attacker vs. an outside attacker***:** An outside attacker may be a passive listener who has no special access to the sensor network, but in case of an inside attacker, this is different as he can access the encryption keys or other codes used in the network. For example, a compromised node in the network could be an insider attacker as it was originally a legitimate part of the sensor network.

Passive vs. active attacker: A passive attacker is only interested in collecting sensitive data from the sensor network, leading to compromising of the privacy and confidentiality requirements. In contrast, the objective of an active attacker is to disrupt the total functionality of the network and there by degrading its performance.

1.4 Attacks On Sensor Networks

Most of the routing protocols proposed for ad hoc and sensor networks are not designed to handle security related issues. Therefore there is a lot of scope for attacks on them. Different possible attacks [5][6][7][9][10][11][12] on the flow of data and control information can be categorized as follows: Flooding attack, HELLO flood attack, Black hole attack, Link withholding attack, Link Spoofing attack, Acknowledgement Spoofing attack, Replay attack, Wormhole attack, Colluding Mis-relay attack, Sybil attack, Sinkhole attack, Energy drain attack, Selective forwarding attack, Partition, Detour, Malign.

Necessary survey has been done on various routing protocols and it has been found that some of routing protocols classified below can be protected against some attacks and but not all.

1.5 Security Objectives And Requirements

In order to achieve security in wireless sensor networks security requirements should be provided. These basic security requirements are as represented in Table 1, system may satisfy some of these requirements depending on applications [6], [9] and [12]. Although security requirements in wireless sensor networks are depending on the application, there are several security requirements which had been proposed by researchers. The selected requirements may be satisfied concerning the application's need.

NAME	DESCRIPTION
Confidentiality	Confidentiality is the ability of hiding message to an unauthorized attacker. It means that the message cannot be understood by any illegal and unauthorized adversary.
Authentication	Authentication is ability to identify the reliability about the origin of the message whether a legitimate node has sent the information.
Integrity	This provides a mechanism to identify the tampering of the message.
Freshness and availability	Availability guarantees the network services on hand. This factor identifies the movement of the message in the network. If the node can use its resource, then the availability is provided to the network for forwarding the message.
Graceful degradation	It is the ability of the network performance to have graceful degradation, when a small portion of nodes are compromised i.e. the designed mechanism must be resilient to node compromise.
Non-repudiation	Sender of the message shall not be able to deny later about the sending of the message and that the recipients shall not be able to deny the receipt after receiving the message.
Resiliency	It is the ability of the network to tolerate the attacks and continue offering its services uninterruptedly.
Self-healing	It is the ability of the network to recover from security problems and even isolate the source of threat so that it stops jeopardizing the availability of the network in future communications.

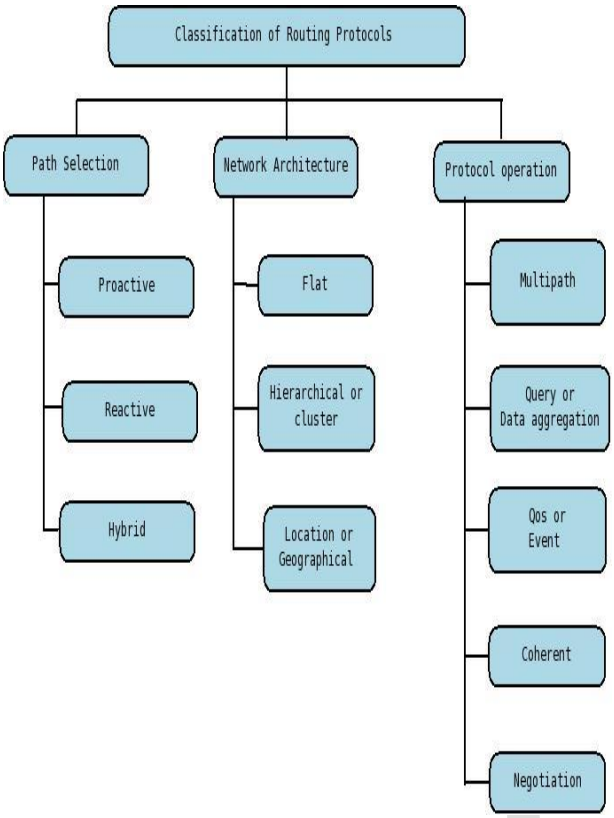
II. CLASSIFICATION OF ROUTING PROTOCOLS

The routing protocols designed for WSN can be classified based on path selection, as proactive, reactive and hybrid as shown in Fig. 2. Based on the network architecture, they can be further classified as flat (data-centric, flat), hierarchical, such as LEACH, TEEN and APTEEN, and geographical information based, such as GAF and GEAR. There are also classifications based on protocol operation, such as multipath-based, query-based, event-driven, negotiation-based and coherent-based.

Fig. 2. Classification of Routing Protocols

Routing protocols for wireless networks can be

classified into three types based on the underlying routing



information update mechanism employed. A routing protocol could be reactive (on demand), proactive (table driven) or hybrid.

2.1 Proactive Routing Protocols

In Proactive or Table driven routing protocols, such as DSDV [21] or OLSR [25], each node in the network periodically exchange the routing information to update their routing table entries and there by maintains the network topology information. Generally, flooding of routing information throughout the network occurs. Whenever a path to destination is needed, an appropriate path finding algorithm is executed by the node on the topology information maintained. Other proactive routing protocols are as follows SEAD, CGSR, STAR, LORA, WRP, GSR, FSR etc.

2.2 Reactive Routing Protocols

Reactive or On-demand Routing Protocols, upon need uses the connection establishment process to obtain the necessary path to destination. They do not maintain the network topology information and exchange of routing information periodically is not required. Reactive routing protocols often outperform proactive ones with their ability to reduce the network overhead created for tracking the mobility in the network. In Reactive routing protocols AODV [19, 24], DSR [22], OLSR [25]and TORA are considered to be most popular routing protocols as many secure versions have been derived from their basic implementation. The analysis of the secure versions of these protocols such as SAODV, SAOMDV, SAR, SQoS, Ariadne, CONFIDANT, ACQUIRE, SPREAD has been investigated.

2.3 Hybrid Routing Protocols

Hybrid Routing Protocols are designed to provide the advantages of both Proactive and Reactive routing protocols. Hibrid Routing Protocols such as ZRP [31] and SLSP [32] combine the best features of both reactive and proactive routing protocols. For example, communication with the neighbors follows a proactive routing protocol, and communication with nodes farther away utilizes a reactive protocol. In other words, for each node, nodes within certain geographical location are reached with proactive routing protocols. Outside the geographical area, reactive routing protocols are used.

2.4 Network Architecture based Protocols

Routing protocols for wireless networks can also be classified into three types based on the built in Network Architecture. The above mentioned routing protocol can be data cetric (flat), Hierarchical (cluster based) or location based.

2.5 Data-Centric Routing Protocols

In data-centric routing, Queries are sent form the sink node to certain regions and data from the sensors is awaited from those selected regions. Since data is being requested using queries, the properties of the data are obtained with attribute-based naming. SPIN [33] is the first data-centric protocol in which redundant data is eliminated by the data negotiation between nodes and hence energy is saved. Later, Directed Diffusion [34] is the next breakthrough in data-centric routing. Then, many other protocols have been proposed either based on Directed Diffusion [34] or following a similar concept [8]. All these protocol are developed with concept of efficient routing kept in mind and does not concentrate on secured routing.

2.6 Hierarchical Routing Protocols

Similar to other communication networks, scalability is a major design attribute in sensor networks. The sink node is overloaded due to heavy increase in sensor data in a single tier network which leads to latency in communication and tracking of events become difficult. It also lacks scalability as they are not capable of long-haul communication. In order to enable the coverage of large area and to manage the additional load, network clustering approach is considered. The prime objective of hierarchical

routing is to efficiently maintain the energy consumption of sensor nodes by involving them in multi-hop communication within a particular cluster and by performing data aggregation and fusion in order to decrease the number of transmitted messages to the sink. Formation of Cluster is typically based on the energy reserve of sensors and proximity of sensor's to the cluster head [35, 36]. LEACH [13] is one of the first hierarchical routing approaches for sensors networks. The idea proposed in LEACH has been an inspiration for many hierarchical routing protocols such as TEEN APTEEN, PEGASIS, Hierarchical PEGASIS[14,15,16,17,18], although some protocols are self configurable systems. Energy aware routing in cluster based sensor networks have been independently developed [8,37,38]. Necessary exploration about hierarchical routing protocols has been done. All these protocol does not concentrate towards secure data communication.

Cluster-based routing protocols group sensor nodes to efficiently relay the sensed data to the sink. The cluster heads are usually chosen as specialized nodes that have less energy-constraints. A cluster-head performs aggregation of data and sends it to the sink on behalf of other nodes within its cluster. The most interesting research issue regarding such protocols is about the formation of clusters so that the energy consumption and contemporary communication metrics such as latency are optimized. The factors affecting cluster formation and cluster-head communication are open issues for future research.

Moreover, the process of data aggregation and fusion among clusters is also an interesting problem to explore. Since the structure of the DODAG in the RPL resembles the same, it is best to choose a hierarchical architecture and add the security primitives with best key distribution mechanism based on symmetric key cryptography.

2.7 Location based or Geographical based protocols

Most of the routing protocols for sensor networks require location information for sensor nodes. In most cases location information is needed in order to calculate the distance between two particular nodes so that energy consumption can be estimated. Since, proper addressing scheme is not available for sensor networks till before the possibility of utilizing IPv6 addressing, location information about the spatial deployment can be utilized for energy efficient routing of data. For instance, if the region to be sensed is known, using the location of sensors, the query can be diffused to that particular region thereby eliminating the number of transmission significantly. MECN and SMECN, GAF, GEAR, Chang and Tassiulas, Kalpakis et. al., Akkaya et. al., SAR, SPEED are some of the Location based protocols. Some of the protocols discussed here are designed primarily for mobile ad hoc networks and consider the mobility of nodes during the design [8,23,26,27,39]. However, these protocols are well applicable to sensor networks considering the immobile nature of the nodes.

Protocols that utilize the information about deployment topology and location of sensor nodes come under the category of location based protocols. The focus towards energy-aware location-based approaches is rather found to be small. The efficient utilization of the location information to aid energy efficient routing is a main research issue but is suitable only for immobile nodes.

Although there is a promising erformance of these protocols in terms of energy efficiency, the focus of research has been diverted to address other issues like multi-path environment protocols posed by real-time applications.

2.8 Multipath based Routing Protocols

In the multipath routing, there exists multiple paths from source to destination and packets travel to destination through these paths. Often, selection of shortest path does not result in reduced network lifetime. Hence, concentration for routing algorithms taking into account multiple sub-optimal paths need to be considered [10,29]. In-network aggregation, the fusion of data from different sources promises to increase network lifetime [40]. The data from the lower levels is combined at the higher levels. There is reduction in packet overhead throughout the network while ultimately communicating the same effective information.

2.9 Energy aware or QoS based Routing protocols

Energy-aware or QoS routing in sensor networks guarantee the QoS parameters such as bandwidth, delay while establishing connection and also provide energy efficient path. QoS routing in sensor networks have several applications including real time battle field target tracking, event triggering in monitoring applications etc. Currently, there is minimum research that handles QoS requirements in an energy constrained environment like sensor networks.

Table 1. Comparison of various routing protocols.

Routing Protocol	Path selection	Network Architecture	Protocol operation	Security
DSDV	a	1	ii	N
OLSR	a	1	ii	N
SEAD	a	1	ii	Y
CGSR	a	2	iii	N
STAR	a	1	iii	N
WRP	a	1	**ii**	**N**
HSR	a	2	ii	N
FSR	a	3	iii	N
DSR	b	1	ii	N
Maltz et.	b	1	iii	N

al.				
SQoS	b	1	iii	Y
Ariadne	b	1	ii	Y
CONFIDANT	b	1	iv	Y
AODV, SAODV	b	1	ii	N,Y
SAR	b	1	iv	Y
TORA	b	2	iii	Y
SPREAD	b	1	i	Y
ARAN	b	1	ii	Y
ZRP	c	1	ii	N
SRP	c	1	ii	Y
CEDAR	c	1	iii	N
ZHLS	c	2 & 3	iii	N
SPIN	b	1	iv	N
Directed Diffusion	b	1	ii	N
Shah and Rabaey	b	1	iii	N
Rumor routing	b	1	ii	N
GBR	-	1	ii	N
CADR	-	1	iii	N
COUGAR	-	1	ii	N
ACQUIRE	-	1	ii	N
LEACH	-	2	ii	N
TEEN	-	2	ii	N
APTEEN	-	2	ii	N
HPEGASIS	-	2	ii	N
Younis et. al.	-	2	iii	N
Subramanian & Katz	-	2	ii	N
MECN & SMECN	-	3	ii	N
GAF	-	2&3	iii	N
GEAR	-	3	iii	N
Chang & Tassiulas	-	2	ii	N
Kalpakis et. al.	-	3	ii	N
Akkaya et. al.	-	2	iii	N
SAR	-	-	iii	N
SPEED	-	3	iii	N
SSPIN	b	1	i	Y
SAOMDV	b	1	i	Y
Jiang & Zhao	b	-	i	Y
Li et. al.	b	3	i	Y
Yao & Zheng	b	-	i	Y
Yin et. al.	b	1	i	Y
STAPLE	b	2	i&ii	Y
Wen et. al.	b	1	i	Y

- **a-Proactive, b-Reactive, c-Hybrid**
- **1 - Data-centric or flat, 2 – Hierarchical, 3 – Location or Geographic based**
- **i-Multipath, ii-Data aggregation or query based, iii-QoS, iv-Negotiation based, v-Coherent based**

In order to generalize the previous findings a matrix is proposed in the Table. 1. It classifies the routing protocols depending on the path selection, Network architecture, protocol operation and has to be chosen depending on the application. In any environment security is the primary issue to be considered, which is also highlighted in the matrix representation. Listed secure protocols address to certain threats, attacks and basic security requirements and not all [30]. Special attention towards the key management schemes for the selected protocols has to be designed with the available security primitives [7].

Another interesting issue for routing protocols is the consideration of node mobility in hostile environments. In the WSN environment, mostly the source and sink nodes are stationary. However, there might be situations such as battle environments where the sink and possibly the sensors need to have mobility. In such cases, the frequent updating of position of the commanding node and the sensor nodes is required and the propagation of that information through the network may excessively drain the energy of nodes. New routing algorithms are needed in order to handle the overhead due to mobility and topology changes in such energy constrained environment. Other possible research issues of routing protocols include the integration of sensor networks with wired networks (i.e. Internet). Most of the

applications in secure environmental monitoring require the data collected from the sensor nodes to be transmitted to a server so that further analysis can be done. On the other hand, the requests from the user should be made to the sink through Internet. Since the routing requirements of each environment are different, further research is necessary for handling these kinds of situations.

III. IMPLEMENTATION OF SECURITY PRIMITIVES

The Sensor motes can broadly be classified depending on the capabilities of the microcontroller used in manufacturing as shown in Table. 2. The selection of a microcontroller depends on the type of services that has to be provided to the node in terms of energy consumption, instruction and RAM memory, storage capacity, speed and external IO ports.

Table. 2. Classification of Sensor Motes based on its characteristics.

Capability	Class I	Class II		Class III	
Model	Atmega168	MSP430 F16x	ATmega128L	PXA271	ARM920T
Frequency	4MHz	8MHz	8MHz	13MHz	180MHz
Word size	8bit	16bit	8bit	32bit	32bit
RAM memory	1kB	10kB	8kB	256kB	512kB
Inst. memory	16kB	48kB	128kB	32MB	4MB
Power (awake)	<1mA	1.8 mA	8mA	31-44mA	40-100mA
Power (slept)	0.1µA	5.1 µA	8µA	390µA	40µA

The hardware platforms chosen for this project are the TelosB and Iris motes which come under the category of Class II type of nodes. Both platforms were originally developed at UC Berkeley and are now produced by the Crossbow Technologies. Both platforms are tiny, low-power motes with restricted resources, equipped with an 802.15.4 RF interface. The Iris mote is similar to other motes, the main difference being a different radio interface AT86RF230 wide band radio. The Iris mote alone does not contain any embedded sensors. However, using the 51-pin extension connector, various sensor boards could be connected. For this project, the MTS 300 sensor board has been available. It contains light, temperature and acoustic (a microphone) sensors as well as a speaker. Other sensor boards with various sensors, such as accelerometers or magnetometers are also available.

While the motes has a USB connector and can directly be plugged into a PC for communication or reprogramming. Clearly, these motes are suitable for low data rate applications requiring only minimum data processing. Spending most of their time in the sleep mode, the motes can run for several years on 2 AAA batteries.

Most of the applications do not need to send large volumes of data through the wireless channel, thus sensor networks will not use the entire bandwidth, and the execution of the cryptographic primitives will not cause a penalty in the communication between nodes. Suffice to say that the high execution time of Public Key primitives, around 2 seconds, limits their use to specific situations such as key negotiation or broadcast authentication. Regarding memory consumption, the class type of a node will determine the amount of memory available to the application logic, including the security primitives. Therefore, this class type will influence over the type of primitives that the node can run. Class III type of nodes have roughly 256kB of RAM and 4MB of instruction memory. These types of sensor nodes are powerful enough to cope with any kind of cryptographic primitives, either symmetric or asymmetric, via software.

On the other side of the spectrum, we can find class I nodes. These nodes, with roughly 1kB of RAM and 16kB of instruction memory, can support software implementations of block cipher algorithms such as AES, RC5, and Skipjack. However, the amount of memory left for implementing the application logic is quite small. Therefore, it may be better to use stream cipher algorithms, whose memory requirements (e.g. 428 bytes of inst. memory for RC4) are still small. Note that, due to extreme memory constraints, these kinds of nodes are not able to execute Public Key Cryptography on software.

Regarding "Class II" nodes, they are the most common hardware platform used on wireless sensor networks. With roughly 4-8kB of RAM and 48-128kB of instruction memory, these nodes are powerful enough to support the execution of any cryptographic primitive on software. Still, considering the actual state of the art, a simple application prototype with support for all the primitives in software will consume 34kB of instruction memory.

From this analysis it is clear that, sensor nodes are capable of running cryptographic primitives such as Symmetric Key Cryptography, Public Key Cryptography, and Hash functions on software. However, the inclusion of hardware cryptographic modules in both "Class I" and "Class II' nodes should be considered, in order to reduce the overhead posed by the implementation of the primitives.

Security primitives, such as Symmetric Key Cryptography (SKC), Public key cryptography (PKC) and Hash function, can provide a secure communication channel between two or more devices with the properties of confidentiality, integrity and authentication, protecting the information flow against any unintended recipients. This is essential to create secure protocols and a secure infrastructure, because no external entities or unintended recipients should be able to manipulate the contents of the messages exchanged by two peers. However, such security primitives need certain security credentials, i.e. secret keys, in order to work. The task of creating and distributing these keys, hence constructing a secure key infrastructure, is done

by the Key Management System (KMS).

Consequently, it is necessary to define the properties that a KMS should have and the requirements of the applications (e.g. network size) that influence over the importance of those properties (e.g. scalability). A Key Management System can be classified by the properties such as memory footprint, processing speed, communication overhead, confidentiality, network resilience, global connectivity, local connectivity, node connectivity, scalability, extensibility, and energy as shown in Fig.3. It is also important to that the requirements of a certain sensor network application influence over the importance of certain properties for that application.

Leaving the basic inefficient methods of key management such as global key establishment and pair-wise key establishment, the other efficient methods in practice can be broadly classified into Symmetric Key Cryptography based Key Management and Public Key Cryptography based Key Management as shown in Fig. . The various schemes in literature spanned under SKC based KMS, can be grouped into Key pool based schemes, Mathematical based schemes and Negotiation based schemes. Each scheme under any of these categories has their own advantages and disadvantages [11].

Mathematical based schemes provide full connectivity inside the sensor network, since every node can calculate by itself the pairwise key that it shares with another node. However, these designs are often difficult to apply, and they are not very scalable: The Linear Algebra and Algebraic Geometry schemes needs a high amount of memory in order to store the mathematical structures and the Combinatorial schemes only work as intended for certain network configurations.

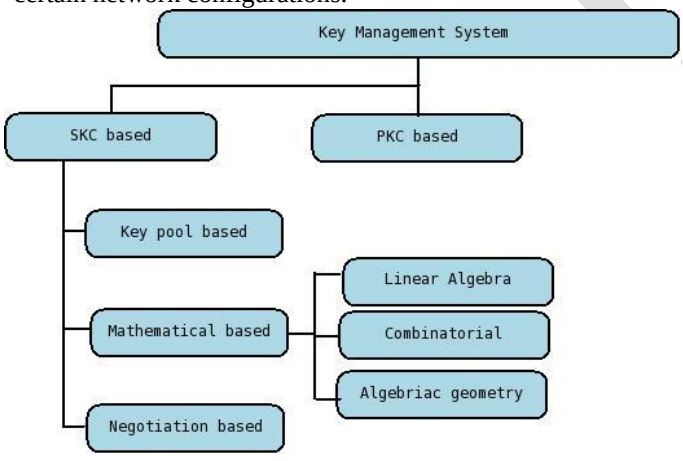


Fig. 3. Classification of Key Management System

In simple, Data centric or flat networks, there is no need to use complex protocols that need of "key pools" or complex negotiations: simple mathematical schemes such as the Blom Key Pre-distribution and Polynomial Key Pre-distribution are enough. On Large Hierarchical networks scalability become a major issue and it is better to use other protocols, such as Dynamic Cluster-based protocols or any "Key Pool" protocol. Scenarios with Mobile Base Stations do not pose a problem, since a sensor node may share a pre-installed pairwise key with that Base Station. As a result, it is possible to use almost any of the protocols utilized on static networks. On the other hand, in networks with mobile nodes, the number of protocols that fulfill their requirements is limited. Nevertheless, Blom and Polynomial Key Pre-distribution may work for small networks, but for bigger networks it may be necessary to use PKC-based protocols.

If speed becomes the primary property, in those networks where mobile nodes must establish a secure channel as fast as possible (almost immediately) with other peers and if extensibility is required, then there is a useful protocol based on generalized Quadrangles which is highly dependent on knowing in advance the maximum number of sensor nodes included inside the network.

Regarding security, if the security of the network during its initial deployment is not that very important, it is possible to use some negotiation-based protocols such as Key Infection in all the groups. For large networks, the redundancy of the network allows to have a tiny fraction of the network disconnected, thus global connectivity can be considered as a secondary property. However, there are some situations where there should be no sensor nodes disconnected from the network. In these situations, global connectivity becomes a main property, and most "key pool" based frameworks cease to be useful. Even more, if extensibility becomes important, very few KMS protocols (mostly those based on mathematical frameworks) can be useful for the network designer.

3.1 6LoWPAN:

Development of IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) architecture enables IPv6 Communication for smart objects over IEEE 802.15.4 links. A new innovation in Internet protocol technology, called 6LoWPAN is making the Internet of Things become a reality. 6LoWPAN is a standard from the Internet Engineering Task Force (IETF) published in 2007, which optimizes IPv6 for use with communication Technologies such as IEEE 802.15.4 radio communication. This is where the embedded systems meet the Wireless Technologies. A modern embedded communication chip consists of transceivers which combine half-duplex transmission and reception with the same hardware. Transceivers integrate varying functionality, from a bare analog interface to whole digital baseband and MAC functions.

The benefits of IP communication and management can be linked with low power devices with the help of 6LoWPAN standard.[3,4] It has a separate adaptation layer, packet format and address management. Each node in the 6LoWPAN network has a unique IPv6 address. 6LoWPAN works by compressing the 60 bytes header down to just 7 bytes with the optimizing mechanism for wireless embedded networking. 6LoWPAN radically alters the calculation by using the adaptation layer that enables efficient IPv6 communication over IEEE 802.15.4

radio links. By installing IPv6 stack to the sensor nodes, the sensor networks have interoperability with the external IPv6 networks [4].

3.2 Routing Protocol - RPL ("Ripple")

IETF proposes a generic framework to control the network layer communication with the help of a routing protocol RPL. RFC 4919 [1] discusses about the assumptions, problem statement and goals for 6LoWPAN, while the adaptation layer for the transmission of Ipv6 packets over IEEE 802.15.4 is described in RFC4944 [2]. RPL provides a mechanism to disseminate information over a dynamically formed network topology. RPL organizes the topology as a Directed Acyclic Graph that is partitioned into one or more Destination Oriented DAGS (DODAGs) with one DODAG per sink. The usages of security mechanisms in RPL are currently undefined and yet open with options for future implementations in the ROLL draft. Therefore the feasibility of employing a suitable secure algorithm with IPv6 is currently an open issue [3]. With this problem in mind and the details of available literature the routing strategy with security by measuring the resource consumption and other critical metric/constraints can be designed.

RPL is a generic framework which can be suited to any type of WSN based on Path selection, Network Architecture and Protocol operation. Also various levels of security can be implemented using RPL, suiting to host any type of application requirement. The Routing protocol comprises of few ICMP layer messages called the RPL control messages. The type of the RPL control message is identified by the 8 bit code field. There a three control messages such as DODAG information solicitation (DIS), DODAG information object (DIO), Destination Advertisement object (DAO), Destination Advertisement object Acknowledge (DAO-ACK), and its secured versions such as SDIS, SDIO, SDAO, SDAO-ACK, and consistency Check (CC) messages. These messages contain information for routing nodes and hosts. The information is gathered to the edge router and routing configurations are sent all over the LoWPAN network. When a node has accomplished Neighbor Discovery, it scans for a DIO by broadcasting a DIS message. When a routing node receives the DIS message, it sends the DIO as a response. The DIO may, or may not, contain DODAG information. The DIO message contains also address information of the parent and a RPL root which is the Edge Router. On reception of the DIO, a DAO is sent to the RPL root after a predefined time. The DAO contains route information from the RPL host to the RPL parent. This information represents one logical interconnection within the simple 6LoWPAN network. When the root receives the DAO, it enters the route information of the DAOs into a routing table. The routing table can be used to build a whole path from the root to the destination node. The nodes can operate in the Storing mode or Non storing mode depending on its capacity to store the routing information. This allows the root to send data to any registered and joined node within a RPL DODAG. As a response to the DAO, DAO-acknowledge is sent if requested. RPL supports three different traffic flows for these messages which could be Point-to-Multipoint, Multipoint-to-Point or Point-to-Point. Usually DIS and DIO can be Multicast or Unicast and DAO and DAO-ACK will be a Unicast communication.

Each RPL messages has its secure variants. The secure variants provide integrity and replay protection as well as optional confidentiality and delay protection. The Security Algorithm field specifies the encryption, MAC, and signature scheme the network uses. The Key Identifier Mode (KIM) is a 2-bit field that indicates whether the key used for packet protection is determined implicitly or explicitly and indicates the particular representation of the Key Identifier field. This facility helps us to have various levels of security depending on the application using the LVL field along with KIM field.

3.3 Implementation of RPL

The implementation of RPL in the unsecured mode has been done over TelosB and Iris motes using nesC language in TINYOS platform. A great interest has been taken up in merging the establishment of secured RPL with the available literature to suit various environments. For example, consider a situation of monitoring elderly persons in a remote location where sensor nodes are deployed around them and the base station is connected to the web server through which the emergency service, care giver and doctor can be linked. It is a simple data aggregation network where the Global connectivity is the primary issue and local connectivity, resilience, security, scalability, Extensibility and node connectivity are secondary properties. For such a network, a standardized secure proactive distance vector routing protocol with dynamic key management scheme can be employed. This can be done by choosing the Algorithm field in the security part of RPL control messages set any value from 1 to 255 indicating a value for each type of encryption algorithm chosen with appropriate option in the KIM field and LVL field with T flag set to indicate the Timestamp counter.

In Military applications, Security becomes the primary issue and scalability, global and local connectivity, extensibility are the secondary properties. A large scale Energy aware hierarchical routing protocol with ECC based KMS scheme can be employed with appropriate choice of Algorithm field set, KIM and LVL with T flag set to indicate the timestamp. For precision agriculture, a simple data-centric proactive data aggregation routing protocol with identifier value can be used in the Algorithm field of the control message with less security. The level of security required differs with the application and the resource availability of the motes under deployment of the scenario.

IV. CONCLUSION

A Standardized secure routing protocol for

6LoWPAN has not been considered so far. The aim of this survey is to envision the various routing protocols and their security mechanisms in literature and emphasis the need to provide a clear definition towards establishment of a security framework for RPL over 6LoWPAN. This could be a valid contribution to the research community and helps to step towards the integration of WSN with Internet of things. With this in mind, several tests and effort has been done taking into account the memory constraints of the available motes deployed for various applications.

REFERENCES

[1.] N. Kushalnagar, G. Montenegro, and C. Montenegro,"RFC 4919 - IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement and Goals," Aug. 2007;

[2.] N. Kushalnagar, G. Montenegro, J. Hui, and D. Culler, "6LoWPAN: Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[3.] S. Daniel Park, et al, "IPv6 over Low Power WPAN Security Analysis," IETF Internet Draft, Feb. 2008.

[4.] K. Kim, et al, "Hierarchical Routing over 6LoWPAN (HiLoW)," IETF Internet Draft, Jun. 2007.

[5.] John P. Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Networks Security: A Survey", book chapter of Security in Distributed, Grid, and Pervasive Computing, Yang Xiao (Eds.), CRC Press, later 2006.

[6.] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Elsevier AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, Sep. 2003, p. 293-315.

[7.] R. Roman, C. Alcaraz, and J. Lopez, "A survey of cryptographic primitives and implementations for hardware constrained sensor network nodes," Mob. Netw. Appl., vo1.I2,2007, pp. 231-244.

[8.] Kemal Akkaya, Mohamed Younis "A survey on routing protocols for wireless sensor networks" Elsevier Ad Hoc Networks Journal 3, 2005, pp.325–349.

[9.] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols" IEEE communications surveys & tutorials, vol. 10, no. 4, 2008, pp. 78-93.

[10.] Ali Modirkhazeni, Norafida Ithni, Sothman Ibrahiecure, "Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis", 2010 Second International Conference on Network Applications, Protocols and Services, Vol 1, pp. 228-233.

[11.] Rodrigo Roman, Cristina Alcaraz, Javier Lopez, Nicolas Sklavos,"Key management systems for sensor networks in the context of the Internet of Things", Elsevier Computers and Electrical Engineering Journal 37, 2011, pp. 147–159.

[12.] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures" Ad Hoc Networks, Vol. 1, 2003, pp. 293–315

[13.] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks," in the Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.

[14.] W. Heinzelman, A.P. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks", IEEE Transactions on Wireless Communications, Vol. 1, No. 4, Oct. 2002, pp.660-670.

[15.] A. Manjeshwar and D. P. Agrawal, "TEEN : A Protocol for Enhanced Efficiency in Wireless Sensor Networks," in the Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.

[16.] A. Manjeshwar and D. P. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," in the Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, Ft. Lauderdale, FL, April 2002

[17.] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power Efficient GAthering in Sensor Information Systems," in the Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, March 2002.

[18.] S. Lindsey, C. S. Raghavendra and K. Sivalingam, "Data Gathering in Sensor Networks using the Energy/Delay Metric", in the Proceedings of the IPDPS Workshop on Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.

[19.] C. E. Perkins and E. M. Royer, "Ad Hoc On-demand Distance Vector Routing," In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.

[20.] Wei Ye, John Heidemann , Deborah Estrin, "An energy efficient MAC protocol for wireless sensor network" 2002.

[21.] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," SIGCOMM, London, UK, August 1994, pp. 234-244.

[22.] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-Hoc Ad hoc Networks," Mobile Computing, ed. T. Imielinski and H. Korth, Kluwer Academic Publishers, 1996, pp. 153-181.

[23.] Y. Xu, J. Heidemann, and D. Estrin, "Geography informed energy conservation for ad hoc routing", Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'01), Rome, Italy, July 2001.

[24.] C. Perkins, Ad hoc On demand Distance Vector (AODV) routing, IETF Internet draft (1997), http://www.ietf.org/internet-drafts/draftietf-manet-aodv-00.txt

[25.] Philippe Jacquet, Paul Muhlethaler, Thomas Clausen, Anis Laouiti, Amir Qayyum, Laurent Viennot, "Optimized Link State Routing Protocol for Ad-Hoc Networks"

[26.] V. Rodoplu and T.H. Ming, "Minimum energy mobile wireless networks," IEEE Journal of Selected Areas in Communications, Vol. 17, No. 8, pp. 1333-1344, 1999.

[27.] L. Li and J. Y Halpern, "Minimum energy mobile wireless networks revisited," in the Proceedings of IEEE International Conference on Communications (ICC'01), Helsinki, Finland, June 2001

[28.] Robert Szewczyk, Alan Mainwaring, Joseph Polastre, John Anderson, "An analysis of a large scale habitat monitoring application", Proceedings of the 2nd international conference on Embedded Networked Sensor Systems, 2004.

[29.] Ali Modirkhazen, Norafida Ithnin, Othman Ibrahim "Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis", Second International Conference on Network Applications, Protocols and Services, 2010.

[30.] Kumar, P.; Cho, S.; Lee, D.S.; Lee, Y.D.; Lee, H.J. "TriSec: A secure data framework for wireless sensor networks using authenticated encryption" Int. J. Marit. Inf. Commun. Sci. (2010), 129-135.

[31.] Z. Haas and M. Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", in IETF MANETS Draft, June 1999.

[32.] P. Papadimitratos, and Z. Haas, "Secure link State Routing for Mobile Ad hoc Networks", IEEE Wksp. Security and Assurance in Ad hoc Networks, 2003.

[33.] J.Kulik, W. R. Heinzelman, and H. Balak-rishnan. Negotiation- based protocols for disseminating information in wireless sensor networks [J]. Wireless Networks, 2002, 8(2/3):169-185.

[34.] C. Intanagonwiwat, R. Govindan and D. Estrin. Directed Diffusion: a scalable and robust communication paradigm for sensor networks[C]. Boston, Massachusetts, USA. ACM. MOBICOM, 2000.56-67.

[35.] A. Buczak and V. Jamalabad, "Self-organization of a Heterogeneous Sensor Network by Genetic Algorithms," Intelligent Engineering Systems Through Artificial Neural Networks, C.H. Dagli, et. (eds.), Vol. 8, pp. 259-264, ASME Press, New York, 1998.

[36.] C.R. Lin and M. Gerla, "Adaptive Clustering for Mobile Wireless Networks," IEEE Journal on Selected areas in Communications, Vol. 15, No. 7, September 1997.

[37.] M. Younis, M. Youssef and K. Arisha, "Energy-Aware Routing in Cluster-Based Sensor Networks", in the Proceedings of the 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems

(MASCOTS2002), Fort Worth, TX, October 2002.
[38.] L. Subramanian and R. H. Katz, "An Architecture for Building Self Configurable Systems," in the Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing, Boston, MA, August 2000.
[39.] Y. Yu, D. Estrin, and R. Govindan, "Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Computer Science Department Technical Report, UCLA-CSD TR-01-0023, May 2001.
[40.] D. Ganesan, et al., "Highly Resilient, Energy Efficient Multipath Routing in wireless Sensor Networks," in Mobile Computing and Communications Review (MC2R), Vol. 1., No. 2. 2002.