International Journal of the Physical Sciences Vol. 6(17), pp. 4245-4254, 2 September, 2011
Available online at http://www.academicjournals.org/IJPS
ISSN 1992 - 1950 ©2011 Academic Journals

Full Length Research Paper

Cross-layer based security solutions for wireless sensor networks

Idrees Sarhan Gawdan[1]*, Chee-Onn Chow[1], Tanveer A. Zia[2] and Qusay, I. Gawdan[3]

[1]Department of Electrical Engineering, Faculty of Engineering, University of Malaya, Kuala Lumpur, 50603 KL, Malaysia.
[2]School of Computing and Mathematics, Charles Sturt University, NSW, Australia.
[3]School of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Andhra Pradesh, India.

Accepted 27 May, 2011

Wireless sensor networks (WSNs) were often used to collect sensitive data and the entire network was particularly vulnerable to various threats at different layers of the protocol stack. With this in mind, there was need to improve security solutions that were inevitable and advantageous to the successful deployment of the wireless sensor networks. The vast research conducted to provide security solutions against various attacks in the WSNs so far was based on the layered approach. In this study, we emphasized that the layered approaches have noticeable shortcomings such as the redundancy and/or inflexibility of the security solutions, which made the layers security solutions often inefficient and inadequate. It was, however, beneficial to construct the security approach for the WSNs based on cross-layer interaction between all components in different layers of the protocol stack. Consequently, these new approaches surely gave a new direction towards the issue of security for wireless sensor networks. The outline of the existing cross layer security schemes in literature was presented, while some new novel security solutions were proposed. More so, the synopsis of the proposed cross-layer based comprehensive security framework (CLBCSF) as the framework model for hierarchical clustering wireless sensor networks was also presented. Nonetheless, the open problems in this area were debated too.

Key words: Immunity cross-layer solutions, wireless sensor networks, layered approach, security, energy efficiency, key management, security framework model, intrusion detection.

INTRODUCTION

Recently, the advances in Nano-technology make it technologically feasible and economically vital to develop low-power battery-operated devices that integrate general-purpose computing with multiple sensing and wireless communications capabilities. We expect that these small devices, referred to as sensor nodes, will be mass produced, making production costs almost negligible. Individual sensor nodes have a non-renewable power supply and once they are deployed, they work unattended. Aggregating sensor nodes into sophisticated computation and communication infrastructures will have a significant impact on a wide range of applications ranging from military, industrial, healthcare and smart homes. The main goal of a WSN is to produce global information from local data sensed by individual sensor nodes over an extended period of time.

These sensor nodes are small in size and have the capabilities to sense and process the data. These sensing capabilities and communicating components of WSNs represent a significant improvement over traditional sensors (Akyildiz et al., 2002). While different aspects of sensor networks have been under intense research, most of the efforts have been considered on network protocols, energy efficiency and distributed data bases (Rabaey et al., 2000). However, few results have been reported in the field of securing WSNs. Security is

*Corresponding author. E-mail: husseinidrees@yahoo.com.

vital when sensor networks are deployed in sensitive applications such as battlefield, premise security and surveillance, and some critical systems such as airports, hospitals, etc. In fact, a network becomes useless without sufficient security mechanisms to protect the integrity and privacy of the data. Though different applications may require different security levels, there are many security requirements, such as availability, authenticity of origin, authentication of data (integrity) and confidentiality (privacy). Details about the security requirement can be seen in Idrees et al. (2010). Nonetheless, Mingbo et al. (2006) added two additional requirements:

1) Survivability: Ability to provide a minimum level of service in the presence of power loss, failures or attacks.
2) Degradation of security services: Ability to change the security level as resource availability changes.

We envision that it is not an easy task to provide an efficient and scalable security solution for WSNs because of their distinguished characteristics, such as vulnerability of channels due to shared wireless medium, vulnerability of sensor nodes in open network architecture, lack of pre-defined infrastructure, changing of network topology in time, harsh and hostile environments, resource limitations of sensor nodes, and dense deployment of nodes over a large area (Yang et al., 2004). Various types of active and passive attacks have been recorded (Idrees et al., 2010; Mingbo et al., 2006):

i. A denial of service (DoS) attack: In DoS attack, a malicious node could prevent another node to go back to sleep mode which in turn causes battery depletion.
ii. Eavesdropping and invasion: If no sound security measures are taken, invasion becomes fairly an easy task due to wireless communication. An adversary could easily extract useful information from the unattended nodes. Hence, a malicious user could join the network undetected by impersonating as some other legitimate node, to have access to secret data, disrupt the network operations, or trace the activity of any node in the network.
iii. Physical node tampering leading to node compromising.
iv. Forced battery exhaustion of a node.
v. Radio jamming at the physical layer.

Since vast quantities of sensor nodes are deployed in the sensor network, the low power and low memory becomes the core design challenge. The low cost constrains the resources that can be implemented on the devices and the low power requires the operations to be done in a highly efficient way. Moreover, due to large scale and deployment nature of WSNs, the proposed protocols and algorithms must be scalable. Recently, a number of solutions have been proposed specifically for securing WSNs (Perrig et al., 2002; Wood and Stankovic, 2002), in that most of the solutions are dealing with attacks on one protocol layer. In this paper, we shall argue that the layered solution is inadequate in security provisioning for WSNs.

A more viable security solution will be the design of a security framework based on cross-layer interplay between all components in different layers of the protocol stack. The framework should comprise much security service components in order to sustain multi-level security services.

FLAWS OF THE LAYERED SECURITY APPROACHES

WSNs interact directly with their physical environments which poses additional security challenges. Subsequently, the existing security mechanisms in the literature are inefficient and inadequate; thus, there is a need to make the WSNs immune to attacks and novel ideas.

We agree with the privileged approach in Mingbo et al. (2006) that the following aspects must be carefully studied when designing cross-layer based security scheme:

i. Adaptive security: The proposed mechanisms have to interact with the environment, and the traffic characteristics can be expected to be different from others. Consequently, we envision that they will require different or at least adaptive security protocols.
ii. Power efficiency: Battery supply is scarce and hence energy consumption is an essential metric to be considered.
iii. Reliability and node density: WSNs have to scale to thousands and hundreds of thousands of nodes, requiring different, more scalable security solutions. Nodes are vulnerable to failures. Unfortunately, the existing security approaches can address only a small, fixed threshold number of compromised nodes, in that the entire security mechanism crashes when the threshold is topped (Ye et al., 2004).
iv. Simplicity: For the fact that sensor nodes are small in size and energy is scarce, the security algorithms must be kept small in storage and size.
v. Nodes do not have a global ID like IP address, owing to the fact that the global ID will add a large amount of overhead due to a large number of sensor nodes.
vi. Self configurability: WSNs will most likely be required to self-configuration into network's status. However, the difference in factors such as traffic and energy trade-offs may require a new approach. Subsequently, some important flaws of the layered approaches would be discussed.

Redundant security provisioning

The prerequisite of maximum security services in each

node may lead to depletion of system resources and may significantly reduce the longevity of the network. The unconsidered design of security provisioning may use up network resources and therefore unintentionally launch security service DoS (SSDoS) attack. Unfortunately, there may be several protocol layers within the network protocol stack which are capable of providing security services to the same attack. Consequently, when the original data go through the protocol stack starting from the highest layer, they will be processed layer-by-layer. To this end, some part of the data packets may go through the security-prerequisite operations of different layers and result in redundant security provisioning.

Inflexible security services

A countermeasure scheme in some protocol layer is unlikely to warrant security provisioning all the time. For instance, link layer security scheme typically addresses confidentiality (data privacy) provisioning, authentication (source and data integrity) and data freshness, but no security issues in the physical layer. However, an insecure physical layer may practically make the entire network remain insecure. So, it is easy to figure out that cross-layer solutions can accomplish better performance. Furthermore, an additional security capability can be achieved via self-adaptive security services, because they are flexible in dealing with the dynamic network topology as well as different types of attacks.

Power inefficiency

The primary concern in designing a sensor network is energy efficiency. There are various sources of power consumption in WSNs, such as idle listening, retransmissions resulting from collisions, control packet overhead, large packet size and unnecessarily high transmitting power. Correspondingly, there are various methods of reducing power consumption. Several approaches limit the transmission power aiming to increase the spatial reuse, while maintaining network connectivity (Wattenhofer et al., 2001). At the medium access control (MAC) layer, the wireless transceivers can be turned off whenever possible, to reduce the idle listening power as well as reducing the number of packets' collisions. At the network layer, an attempt was made to construct power awareness routing protocols to improve significant power savings (Aslam et al., 2003). Depending on the specific applications, measures can be taken at the application layer to reasonably improve power consumption (Madden et al., 2002).

Yu and Guan (2005) aims to drastically reduce the number of potential neighbors of each node, as an attempt was made for reducing unnecessarily power consumption of every node within the network. From all the aforementioned measures, we quite agree with Min et al. (2002) where the issue of power efficiency design cannot be considered completely at any single layer in the networking stack.

CROSS-LAYER BASED SECURITY SOLUTIONS

According to the guiding principles in Jones et al. (2003) for dealing with the issues of securing WSNs, the security of a network is determined by the security it has over all the layers, which in effect is the main concept of cross-layer security solution. However, it should be recalled that a security based on layered design is often inefficient and inadequate. Furthermore, a highly secure mechanism inevitably often uses up a large amount of system resources. Consequently, it may unintentionally launch SSDoS attack as we mentioned in redundant security provisioning. We believe that the cross-layer design is a unique candidate to provide a better security solution. For instance, the energy-efficient security approach has to take cross-layer interplaying into consideration, such as energy issue being a physical layer parameter, and security provisioning being an application layer service.

Reviewing cross-layer design mechanisms

In effect, cross-layer security design no longer gains significant attention by the community researchers. So far, there are only a few schemes that consider factors from different protocol stacks. Here, we reviewed some categories of a typical mechanism. The first category is the key management mechanism. A cross-layer design approach is introduced in Lazos and Poovendran (2004) where a key management mechanism in wireless multicast is proposed. With this approach, secret keys to valid group members are deployed in an energy-efficient way. Authors considered the physical and network layer in combination.

Eschenauer and Gligor (2002) propose a cross-layer based sub-optimal algorithm that considers the node transmission power (physical layer property) and the multicast routing tree (network layer property) to construct an energy-efficient key distribution management (application layer property) and minimize the energy required for rekeying. As such, a cross-layer based algorithm for multicast key distribution that exploits routing energies from the sender and Hamming codes representing the paths from the sender to each node in order to minimize the average energy for rekeying is presented in Lazos et al. (2004).

A novel solution was proposed in Jones et al. (2003) merging parameterized frequency hopping and secret keys in a unified framework, as an attempt to provide differential security services for WSNs. This approach supports a differential security service in places that are

dynamically configured to accommodate updating and may occur for both changing application and network system state.

A Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol, proposed in Melodia et al. (2005), alleviates internodes interference which also reduces per-hop delay through cross-layer interplays with the network layer. The suboptimal algorithm is based on a cross-layer approach through collecting the corresponding information from the Physical PHY and MAC layers.

Also, there are cross layer implementations for power management schemes and path redundancy based security as observed in Sami and Eng (2007). Bhaskaran and Kameswari (2008) pointed out that WSNs protocols are deeply dependent on application scenarios, but most of the protocols do not use any specific application in its design. So, recent security schemes also lack security provisioning to specific scenarios while assessing their security needs. Tae and Hee (2008) give a simple trust model, utilizing fuzzy logic that addresses the secure routing problem. The model calculates the evaluation value for each path and ensures that packet is always forwarded to a high evaluation value path. A mechanism for prohibiting the compromised node to become the cluster head is introduced in Garth et al. (2006) which is based on trust factor and some initiatives to support security framework. Thus, this integrates two or more security schemes like secure cluster formation, key management, etc. It sustains holistic approach to provide security. The main problem with the holistic security approach is that it relies on the security layer which results in redundant security. Thus, holistic approach based securing sensor networks were recommended in order to achieve securing multiple layers in the protocol stack by exploitation of the interaction between security measures in various layers to provide a satisfactory security service for the entire network.

Novel directions toward cross-layer approach

Each protocol layer notably emphasizes different aspects for the security provisioning in WSNs. The physical layer provides information privacy using encoding. The link and network layers deal with the encryption of sensitive data and routing information. The application layer (higher layer in the protocol stack) focuses on key management mechanism and rekeying, which in turn supports encryption and decryption of the lower layers. When considering the security issue of sensor networks, we must be aware of the characteristics of each layer, then construct a cross-layer approach to trade security off network performance and alleviate as much redundancy as possible. Mingbo et al. (2006) clarified the concept of cross-layer, through the next example. If the objective is to provide energy-efficient security provisioning, we may integrate the following techniques:

1. At the physical layer, transmission power can be automatically tuned according to the interference strength, which alleviate energy consumption and strive to congest attacks.
2. At MAC layer, we can reduce the number of retransmissions' packets, which in turn restrain exhaustion attack and saves energy as well.
3. At the network layer, we can adopt multi-path routing, which bypasses routing black-hole and alleviates the energy consumption due to congestion.

However, we can contrive that one vital approach to develop cross-layer based security mechanism individually for various categories of security issues.

Cross-layer security for heterogeneous requirements and service types

A sensor network may comprise different types of sensors and implement multiple concurrent applications. Different application scenarios will have diverse security requirements. Even within the application itself, each individual task may have different security concerns. Slijepcevic and Potkonjak (2002) classified the types of data transferred into the sensor networks, identified the possible communication security threats according to that classification and presented a multi-tiered security architecture, thereby achieving an efficient resource management. A link layer Secure Sense was presented in Qi and Ganz (2003) in order to provide energy-efficient secure communication in WSNs. Using runtime security service composition, Secure Sense enables a sensor node to optimally allocate its resource to suitable security services, relying on observed external environments, internal constraints, and application requirements.

We envision that the aforementioned techniques have considered different security issues for different requirements and services. However, they have not considered the fact that variances of these services or requirements may also be reflected at various protocol layers. The security overhead and energy consumption added by security mechanism must correspond to the sensitivity of the encrypted information. We can designate the security requirements to various layers, in order to minimize the security-related energy consumption factor.

Cross-layer security design for intrusion detection

All approaches pertaining to intrusion detection schemes have been focused on routing and MAC protocols. The existing secure protocols or intrusion detection schemes are normally presented for one protocol layer. So, the effect of these schemes is sandwiched to attacks to a particular layer. They are seldom effective to attacks from

different protocol layers; however, security concerns may arise in all protocol layers. It is necessary to have a cross-layer based detection framework that consolidates various schemes in various protocol layers. None of the existing protocols has really taken into account cross-layer architecture for intrusion detection, though a preliminary framework was introduced in Zhang and Lee (2000).

We also necessitate to note that some existing approaches for one protocol layer are not well done; for instance, the general assumption that MAC is for one-hop connectivity (Akyildiz et al., 2002), where it may actually not be true in WSNs. Consequently, such security schemes based on such assumptions may turn out to be obsolete in future WSNs. Also, Intrusion in the physical layer has always been ignored by researchers. However, this type of attack is much more serious and very hard to detect. Malicious users may intentionally jam the wireless channel; in such a situation, security detection schemes based on MAC or routing protocols are unlikely to find out the issue. To the best of our knowledge, many research issues still stay for intrusion detection techniques at various protocol layers.

Cross-layer security design for power efficiency

As previously mentioned, energy conservation is one of the primary concerns for sensor networks' design, so it should be considered across protocol layers from the beginning stage through subsequent stages of the design to achieve the tradeoff between energy consumption, network performance and complexity, and maximize the longevity of the entire network. Our cross-layer approach can achieve this while providing network security provisioning. For instance, the carrier detection is responsible for DoS attacks. A detrimental and\or malicious node can exploit the interplays in MAC layer to frequently request for channels. This not only prohibits other nodes from connecting with the destination, but also can deplete its battery energy due to frequent responses. To overcome this issue, the information can be collected from other layers and the detrimental node can be recognized and then be limited or isolated.

Additionally, at the network layer, we may choose proper route utilizing information from other layers. For instance, from the two-party authentication information, we may choose a route to bypass a malicious node or an attacked area. From the information of battery usage, we may choose a node with more energy left to perform more computational load for security issue or to relay more traffic. Also, the geographical location information can help to attempt attacks, such as Sinkhole. Cross layer solutions for 'energy efficiency' are also being achieved in cooperation of physical layer, link layer and Network layer (Mingbo et al., 2006; Ayman et al., 2010). However, the 'cross layer security solution' is still known to be an unexplored field.

We suggest that the safest and most energy-conserving node is the inactive node, (that is, the node in sleeping). As such, various node-sleeping mechanisms should be exploited as much as possible.

Cross-layer design for key management scheme

Owing to resource limitations of sensor nodes, we strongly recommend to save storage space, decrease the computational needs and reduce communication overheads for key management design. Enormous and different key management mechanisms exist in literature, such as Basic Random Key Scheme (Eschenauer and Gligor, 2002) and Polynomial Poll Based Key Scheme (Du et al., 2003). Of course they vary in scalability, complexity and activity in resisting cracking. Adaptive key management scheme must be devised to consider information such as security level, congestion, location and the remaining energy. We strongly support the approach in Mingbo et al. (2006) that one important task is to derive the overall optimization subject to constraints across multiple protocol layers. The suggested key management scheme based on such an optimization algorithm in turn needs to have various components located at multiple layers to work reactively to really deliver the overall optimized performance.

Cross-layer security design for detecting selfish nodes

One of the common issues in WSNs is that if one node intentionally stops forwarding packets to its neighbors that part of the network will eventually become out of service. In effect, there are two approaches to this issue in WSNs:

1. We suggest monitoring mechanism in the communication protocols to guarantee a node that has enough interest to forward packets to its neighbors.
2. We also suggest developing detection mechanism for the communication protocols to detect selfish nodes, warn or penalize them when detected and lead them back to the proper collaboration mode.

To the best of our knowledge, there is need to notice that both approaches heavily rely on cross-layer design methodology, since selfish behavior can come out from any protocol layer, in particular, MAC and routing protocols. When cross-layer design methodology is deploying to the network with existence of such selfish node, certain actions can be taken by the component in the MAC layer. Such a scheme can detect a selfish node more quickly, due to the faster actions of a MAC protocol than a networking protocol. We contrive that this cross-layer

architecture also alleviate the communication overhead when compared with a standard one-layer approach that gives more robustness to selfish behavior.

Cross-layer based security framework for wireless sensor networks

So far, most of the existing solutions have come up with security solution to WSNs based on the layered design. These layered approaches have salient defects like redundant security and\or inflexible security solutions. We envision that there is strong need to design a novel security framework based on the concept of cross layer design methodology. This framework may support many components like Intrusion detection system, Trust framework, Key management scheme and Adapted link layer communication protocol. The proposed framework model will be presented subsequently.

In effect, in order to carry out practical cross-layer based security framework, the following design guidelines are adhered to (Kalpana and Ghose, 2011, 2009):

1) Component based security: Security measures must be provided to all the components of a protocol stack as well as to the entire network. The developers should focus on securing the entire network.
2) Robust, simple and flexible designs: Security mechanisms should construct a trustworthy system out of untrustworthy components and have the capability to detect and function when need arises. This should also support scalability.
3) Adaptive security: WSNs have numerous combinations of sensing, communication and computing technologies, and sensors are deployed from very sparse to dense quantities. So, relying on traffic characteristics and environment, they have to adapt to themselves. In other words, the sensor network should adapt them according to the outside environment. The notion of adaptive security is further categorized into the following sub-categories:

i. Underlying application based: Each application demands different levels of security. The goal of this framework is the development of the specific security framework application.
ii. Data based: Security level relies on the type of data. For instance, there should be various levels of encryption for routing, sensed data, control packet data and encryption key information.

Kalpana and Ghose (2011) discussed the noticeable features of their framework, cross layer integrated frame-work for security for WSNs (CLIFFS), with the aid of an added extra component called intelligent security agent (ISA) which is liable for assessing the level of security and cross layer interplays. The coupling of ISA with the node protocol stack is depicted in Figure 1.

Also, an integrated security framework has been presented by Tanveer and Albert (2006) in which the solution provisioning is at par with the best and the authors have compared the results with the de facto standard for the link layer security TinySec (Karlof et al., 2004). We notice that this solution is holistic, which means that security provisions prove to be overdone if it is to be implemented with various application domains of WSNs, such as cultural farming in which security issue is no longer needed. The framework approach does not claim to be inviolate to all the security threats, but this surely gives a new direction towards the security issues of the WSNs.

THE PROPOSED CROSS-LAYER BASED COMPREHENSIVE SECURITY FRAMEWORK FOR WSNS

All proposed cross-layer based security solutions are compatible to all existing topologies for WSNs. Here, we present one of the most interesting topologies for recent researches, that is, Hierarchical cluster formation.

We envision that the single layer security solution is often inefficient and inadequate for provisioning secure data transmission in WSNs. So it is, however, beneficial to construct the concept of security framework approach for the WSNs based on cross-layer interaction between all components in different layers of the protocol stack.

This study aims to break with the conventional layering rules and propose cross-layer based comprehensive security framework (CLBCSF) as a security framework model for hierarchical cluster wireless sensor networks. This novel framework is based on cross-layer interaction between all components in different layers of the protocol stack. It comprises Hierarchical cluster formation module, Novel key management module and Network state-based secure communication protocol. The coupling of these modules with wireless sensor networks is depicted in Figure 2.

Hierarchical cluster formation module

This module is an advanced version of hierarchical clustering to overcome the drawbacks of the well known existing protocols so far for WSNs such as routing protocols presented in Heinzelman et al. (2000, 2002). However, these typical protocols have drawback of unequal energy depletion in cluster heads (CHs) due to the different transmission distance from each CH to the base station (BS). In this module, we propose the selection of super cluster head (SCH) among CHs depending on its distance from the BS, which is definitely based on its location and the decision on the number of CHs within the network based on the number of nodes

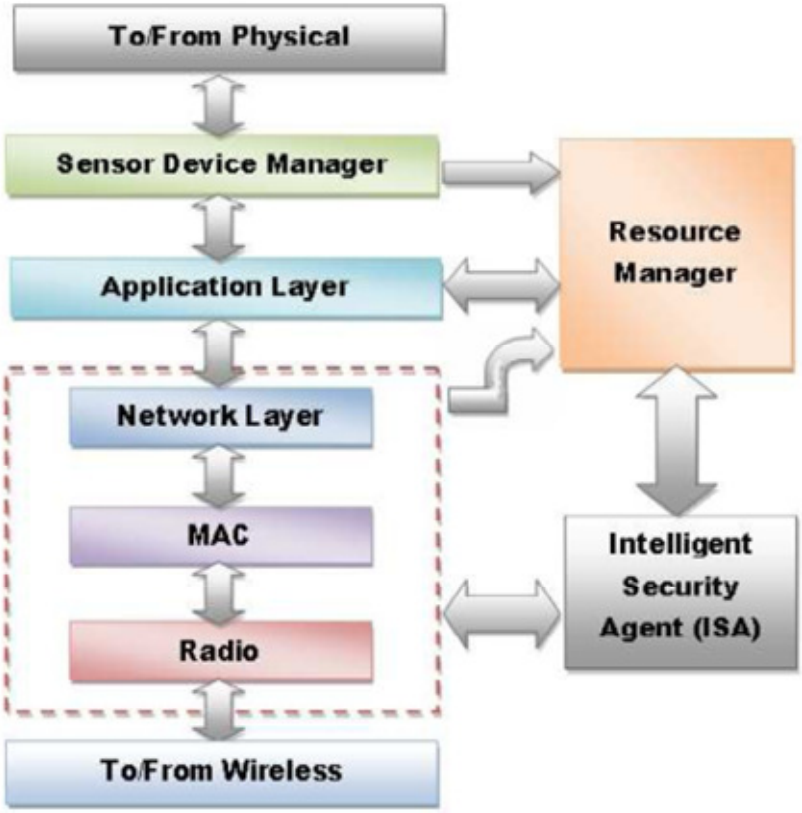

Figure 1. Coupling of ISA with protocol stack (Kalpana and Ghose, 2011).

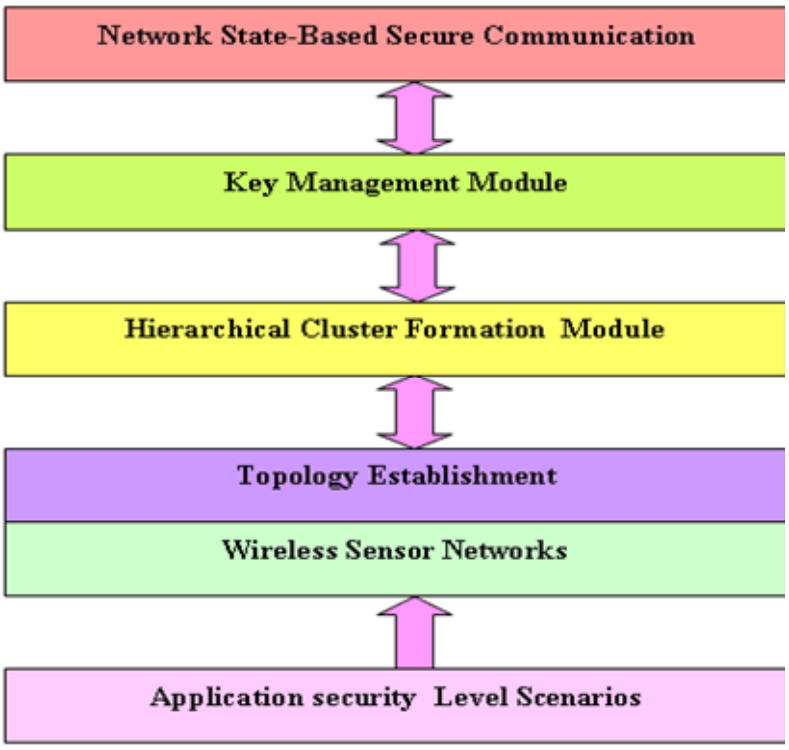

Figure 2. Cross-layer based comprehensive security framework for WSNs.

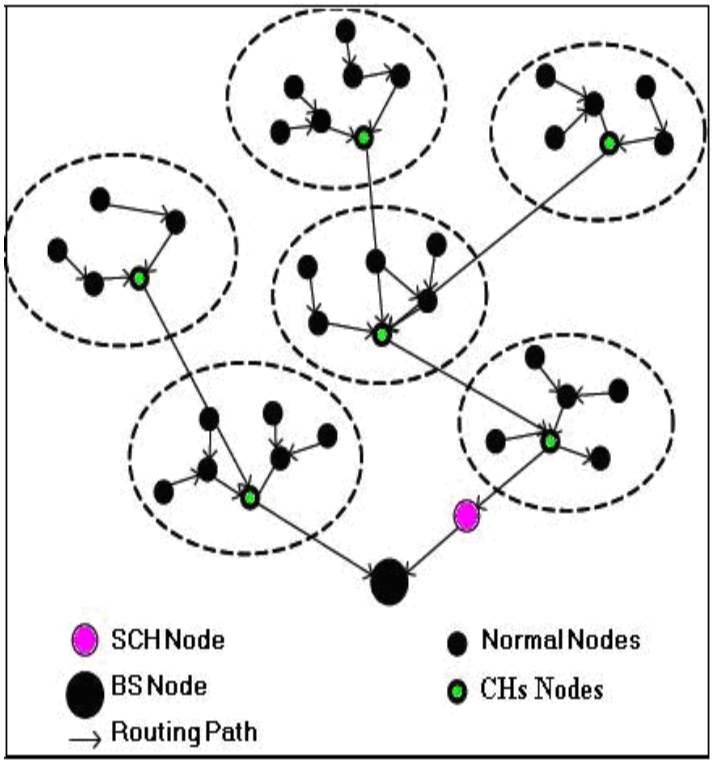

Figure 3. Hierarchical cluster formation module.

that are still alive in every round. Already, the trust module for calculation of trust levels for all nodes exists in the network, and all steps are secured. The node member sends sensed data to CHs, while the CHs, in turn, send its aggregated data to SCH or BS if its location is closest to BS. This leads to the avoidance of more energy consumption. Consequently, our module surely gives a new direction towards saving energy for such starved resources sensor nodes. The hierarchical cluster formation module exploits the advantages of both centralized and decentralized properties of WSNs as depicted in Figure 3.

Novel key management module

This module is responsible for creation, distribution and maintenance of the secret keys by periodically renewing its keys to strive likely to compromised nodes. Thus, the secret keys that will be proposed in the entire network are:

i. Master key (K_M): This, which is a preloaded key to all nodes before deploying, will be used to secure communication data in the setup phase, and must be deleted after setup phase.
ii. Guest key (K_G)): This is a preloaded key and will be used by a new node added to achieve scalable network.
iii. Cluster key (K_C): This key is used to calculate every node within a particular cluster for broadcasting communication between members and securing data to be sent to their CH.
iv. Super cluster key (K_{SC}): This key is used to calculate BS and is held by SCH and CHs nodes only for a particular round.

Key management scheme is the task of the application layer, which is aware of the location of all nodes, energy and TX power of the radio module for all nodes within the entire network. Thus, the radio module function is the task of the physical layer (that is, there are interplays among layers of the protocol stack). Actually, this is the core interplay of the cross-layer approach.

Network state-based secure communication protocol

So far, none of the existing protocols provide adaptive security link layer scheme which dynamically adjusts itself to a particular security level relying on the network state. We prefer using the symmetric key than the asymmetric key in the encryption technique, since the asymmetric key will add the computational overheads about three times more than the symmetric key. The proposed security level is to be implemented by the link layer protocol depending on the application type scenarios and

data type. For instance, agriculture farming and military surveillance system are the popular WSNs applications. In the case of agriculture farming, only data integration using hushing functions check can be utilized, while military surveillance system needs strict security services such as encryption, authentication and strong resilience to compromise node attacks. The correct decision for the level of security largely depends on the correct predefined policies and recommendations. If the network being used is in an agricultural specific scenario, then it should be specified during the time of deployment in order to instruct the link layer to fine-tune itself to the security level fit for the underlying application.

Secure routing protocol module

This module is responsible for the communication of base station with other nodes of the network through super cluster head (SCH) and trusted cluster heads (CHs). It incorporates all the aforementioned modules with effective, energy efficient, distance awareness and dynamic clustering into the routing protocol based on cross-layer interplaying parameters among all layers of the protocol stack as depicted in Figure 3. This will definitely give a new direction toward securing WSNs and elongating the lifetime of the entire network.

DISCUSSION

The theory that was presented by this work takes its inspiration from the concept of cross-layer design for wireless sensor networks. This concept takes a strong and important role to build a right decision about the security issues of provisioning.

The vast research conducted to provide security solutions against various attacks in the WSNs so far is based on the layered approach. In this work, we contrive that the layered approaches have noticeable flaws such as the redundancy and\or inflexibility of the security solutions, which makes the existing layers security solutions often inefficient and inadequate. With this in mind, it is, however, beneficial to construct the security approach for the WSNs based on cross-layer interplay between all components in different layers of the protocol stack. Consequently, this new approach surely gives a new direction towards the issue of security for wireless sensor networks. The explanation and the results of this work will confirm that inspiring the cross-layer design will improve the Security services provisioning of the entire network, performance efficiency and saving of energy to a large extent.

CONCLUSION

In this paper, a novel idea of security solutions for WSNs was proposed. The concept of cross-layer based security framework for WSNs was proposed as an adaptive security solution for various application scenarios, which in turn lead to saving of energy to a large extent. The cross-layer based solutions are anticipated to be the choice solution to closely introspect the tradeoff between added security overhead, vulnerability and network performance. Incorporating the proposed CLBCSF frame-work with effective, energy efficient, distance aware and dynamic clustering secure routing protocol, based on cross-layer interplaying parameters among all layers of the protocol stack, forms the appropriate framework model for hierarchical clustering WSNs as shown in Figure 3. This will definitely give a new direction towards securing the communication links and elongating the lifetime of the entire network. Also, it will be crucial to provide security services to each layer and the services of the entire WSNs.

ACKNOWLEDGMENTS

The authors thank the University of Malaya for providing the research grant PS134/2010A to support this research work. The corresponding author wishes to thank the Ministry of Higher Education of Kurdistan Regional Government, Iraq for the awarded scholarship he used to pursue his PhD abroad.

REFERENCES

Akyildiz IF, Weilian Su, Sankarasubramaniam Y, Cayirci E (2002). A survey on sensor networks. IEEE Communications Magazine, 40(8): 102-114.

Aslam J, Li Q, Rus D (2003). Three power-aware routing algorithms for sensor networks. WCMC, 2 (3): 187-208.

Ayman K, Matthieu C, Jean-François H (2010). Cross Layer Resource Allocation Scheme under Heterogeneous constraints for Next Generation High Rate WPAN. IJCNC, 2(3).

Bhaskaran R, Kameswari C (2008). Sensor Networks: A Critique of “Sensor Networks” from a Systems Perspective. ACM SIGCOMM Computer Communication Review 38(3).

Du W, Deng J, Han YS, Varshney PK (2003). A Pairwise Key Pre distribution Scheme for Wireless Sensor Network. In ACM CCS: 42-51.

Eschenauer L, Gligor VD (2002). A Key-Management Schemes for Sensor Networks. The 9th ACM CCCS: 41-47.

Garth V, Niki P, James G (2006). A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks. Proc. Second IEEE Workshop (DSSNS'06).

Heinzelman W, Chandrakasan A, Balakrishnan H (2000). "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proceedings of the 33rd Hawaii Int. Conf. Syst. Sci., (HICSS '00): 3005–3014, January.

Heinzelman W, Chandrakasan A, Balakrishnan H (2002). An application-specific protocol architecture for wireless microsensor networks. In EEE Transactions on Wireless Communications, TWC: 660–670, October.

Idrees SK, Chee-Onn C, Hiroshi I, Tanveer AZ (2010). Threat Models and Security Issues in Wireless Sensor Networks "proc. (ICINC 2010), 1: 384-389. Kuala Lumpur, Malaysia.

Jones K, Wadaa A, Oladu S, Wilson L (2003). Towards a New Paradigm for Securing Wireless Sensor Networks. In Proceedings of the 2003 workshop on NSP: pp. 115-121.

Kalpana S, Ghose MK (2009). Complete Security Framework for Wireless Sensor Networks. IJCSIS 3(1).
Kalpana S, Ghose MK (2011). Cross Layer Security Framework for Wireless Sensor Networks. IJSA, 5(1): 39-52.
Karlof C, Shastry N, Wagner D (2004). TinySec: link layer security architecture for wireless sensor Networks. SenSys'04, Baltimore, Maryland, USA.
Lazos L, Poovendran R (2004). Cross-layer design for energy-efficient secure multicast communications in ad hoc networks, Communications. IEEE IC, 6(20-24): 3633-3639.
Lazos L, Salido J, Poovendran R (2004). VP3: Using vertex path and power proximity for energy efficient key distribution. VTC2004-Fall. IEEE, 2: 1228-1232.
Madden SR, Franklin MJ, Hellerstein JM, Hong W (2002). TAG: a Tiny Aggregation service for ad-hoc sensor networks. Proc. OSDI, 2002.
Melodia T, Vuran MC, Pompili D (2005). The state of the art in cross-layer design for wireless sensor networks. Proceedings of Euro-NGI Workshops on Wireless and Mobility, Springer, LNCS 388, Como, Italy.
Min R, Bhardwaj M, Ickes N, Wang A, Chandrakasan A (2002). The hardware and the network: Total-system strategies for power aware wireless micro-sensors. Proc. IEEE CAS Workshop on WCNP.
Mingbo X, Xudong W, Guangsong Y (2006). Cross-Layer Design for the Security of Wireless Sensor Networks. Proceedings of the 6th WCICA.
Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD (2002). SPINS: Security protocols for sensor networks. In Wireless Networks, 8(5): 521-534.
Qi X, Ganz A (2003). Runtime security composition for sensor networks (SecureSense). VTC 2003-Fall, 5: 2976-2980.
Rabaey J, Ammer J, Silva JL, Patel D (2000). PicoRadio: Ad hoc Wireless Networking of Ubiquitous Low-Energy Sensor/Monitor Nodes. Workshop on VLSI: pp. 9-14.
Sami SW, Eng SAA (2007). PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Networks. WCNC Proceedings: 4159-4163.
Slijepcevic S, Potkonjak M (2002). On Communication Security in Wireless Ad-Hoc Sensor Networks. Eleventh IEEE International WETICE, 1(1): 139-144.
Tae K, Hee SS (2008). A Trust Model using Fuzzy Logic in Wireless Sensor Network. Proceedings of world academy of science, engineering and technology volume 32.
Tanveer Z, Albert Z (2006). A Security Framework for Wireless Sensor Networks. IEEE-SAS, Houston, Texas USA.
Wattenhofer R, Li L, Bahl P, Wang YM (2001). Distributed topology control for power efficient operation in multi-hop wireless ad hoc networks. Proc. INFOCOM: pp. 1388-1397.
Wood AD, Stankovic JA (2002). Denial of service in sensor networks. IEEE Comput., 35(10): 54-62.
Yang H, Luo H, Ye F, Lu S, Zhang L (2004). Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications, 11(1): 38-47.
Ye F, Luo H, Lu S, Zhang L (2004). Statistical en-route filtering of injected false data in sensor networks. In INFOCOM.
Yu Z, Guan Y (2005). A robust group-based key management scheme for wireless sensor networks. IEEE WCN C, 4: 13-17.
Zhang Y, Lee W (2000). Intrusion Detection in Wireless Ad-Hoc Networks. ACM MOBICOM: pp. 275-283.