SECURITY IN FUTURE MOBILE SENSOR NETWORKS
Issues and Challenges

Eliana Stavrou, Andreas Pitsillides
Department of Computer Science, University of Cyprus, P.O. Box 20537, Nicosia, Cyprus

George Hadjichristofi, Christoforos Hadjicostis
Department of Electrical and Computer Engineering, University of Cyprus, P.O. Box 20537, Nicosia, Cyprus

Keywords: Sensor networks, Security, Routing, Key management, Trust management.

Abstract: Existing security research in wireless sensor networks is based on specific assumptions about the nodes and the network environment that are tied to specific usage scenarios. Typical scenarios consider sensor nodes that are immobile and have pre-defined communication patterns. We argue that node mobility is a realistic characteristic of sensor nodes that needs to be taken into consideration in future sensor networks. Mobility capabilities can address the objective challenges raised in mission-critical applications, such as in disaster relief, where their environment characteristics fluctuate over time. It is imperative to investigate the way security is affected in mobile sensor networks and identify the challenges that will need to be addressed in future security protocol design. We present our vision for future sensor networks through a realistic scenario and discuss security gaps that are present in existing research for next generation sensor networks.

1 INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged in a number of mission-critical application domains (Garcia-Hernandez, Ibarguengoytia-Gonzalez and Perez-Diaz, 2007), such as in healthcare, military surveillance, and disaster mitigation and response. The data sensitivity and the variability of attacks (Chan and Perrig, 2003; Karlof and Wagner, 2003; Wood and Stankovic, 2002, 2004) that can be launched against a WSN have led researchers into investigating a number of security aspects in WSNs and proposing appropriate security protocols. So far, research has been focused on investigating security aspects in static WSNs. However, a radical shift in the way WSNs are studied, designed, and deployed is expected, since mobility features are starting to emerge. For example, in large deployment areas, it is often expensive to deploy sensor nodes to cover the entire monitoring area. Similarly, in mission-critical applications a number of attributes are required to be monitored. For such reasons, (and due to the sensor nodes' constraints), having a node monitor all required attributes is not be feasible. Instead, it is preferable to deploy sensor nodes with different sensing capabilities that can go mobile under specific conditions providing in this way dynamic monitoring coverage.

Mobility is not an unrealistic or undesirable characteristic of sensor nodes as it can address the objective challenges raised in mission-critical applications. For example, disaster mitigation and response (DMR) applications, e.g. fire monitoring, aim to effectively and efficiently prevent hazards or reduce the effect of disasters when they occur. The mobilization of sensor nodes in DMR can support the proactive and reactive emergency services and also the communication of the emergency crew. New challenges that have not yet been investigated in the literature arise due to a number of reasons such as: 1) the nature of disasters, e.g., fires, which include a number of parameters that need to be taken into consideration when implementing DMR applications, and 2) these parameters can dynamically drive the spread and impact of disaster in unpredictable ways. Thus, realistic mobility-based scenarios with WSNs need to be taken into consideration in order to address these challenges

Stavrou E., Pitsillides A., Hadjichristofi G. and Hadjicostis C. (2010).
SECURITY IN FUTURE MOBILE SENSOR NETWORKS - Issues and Challenges.
In *Proceedings of the International Conference on Security and Cryptography*, pages 278-286
DOI: 10.5220/0002987302780286

and also to investigate the way security is being formed/affected in sensor networks where nodes go mobile.

This research work identifies a new mobility-based fire monitoring scenario, utilizes it to study security issues and requirements that arise due to node mobility, and provides directions for future security protocol designs in WSNs.

2 SYSTEM REQUIREMENTS

In this section we discuss our vision for the requirements of next generation WSNs through a real life scenario. WSNs have been successfully deployed in a number of environmental applications. A potential (realistic) forest fire-monitoring scenario considers both fixed and mobile nodes to help the user visualize the application domain.

A WSN-based forest fire-monitoring application has a number of objectives that must be supported by the sensor nodes operation and collaboration, such as detecting and reacting to a fire in a timely manner, effectively controlling the damage, detecting arsonists, and promoting the emergency team's safety and collaboration.

In our scenario, we consider multiple sensor nodes that move around in an area to collect specific information regarding the environment and support the application's objectives. In Figure 1, we depict the WSN forest fire-monitoring application where the sensor nodes are categorized according to their capabilities/functionality. Sensors of type 1 which monitor temperature and humidity, and can detect smoke, are deployed around the forest edge. Sensors of type 2 monitor wind speed and direction and are spread within the deployment area. Sensors of type 3 monitor motion and are equipped with cameras. Sensors of type 4 are deployed on the helmets of the emergency team and have type 1 and 2 sensing capabilities. Sensors of type 5 are coordinators, supporting connectivity between sensor nodes. The data collected by a sensor of a specific type can drive the moving patterns and behaviour of other nodes. For example, when smoke is detected by type 1 nodes, sensors of type 3 are queried to send a picture to the sink. If type 3 sensors are not in the area, they are instructed to move towards the infected areas.

Each node maintains routing paths to a control centre, called the Base Station (BS) or sink, where the observations are been forwarded for further processing and decision making. Initially, the sensor nodes move to predetermined locations based on their sensing capabilities, where specific observations are required. We assume that the emergency team studies the deployment area and plans how the sensor nodes of specific type are spread to cover the area as required and support the aforementioned application objectives.

After the network is deployed and sensor nodes have moved to their initial location defined by the emergency team, communication is established among the nodes to support their activities. Nodes must then have the capability to patrol the area and collect the various data as well as adjust to possible changes in the coverage area, such as in the case of a falling tree (see Figure 1). Thus, compared to previously studied scenarios, the network is reformed dynamically based on the observations and event detections. This reformation implies that the WSN establishes a number of communication patterns to support the collaboration of nodes that are listed under the same or different category.

Summarizing, based on our aforementioned scenario, we envision the existence of mobile sensor networks that will utilize more complicated communications patterns compared to the typical source to BS communication. Moreover, they will be required to adjust to changing areas of coverage while being constrained by energy. Our focus in this paper is on security aspects.

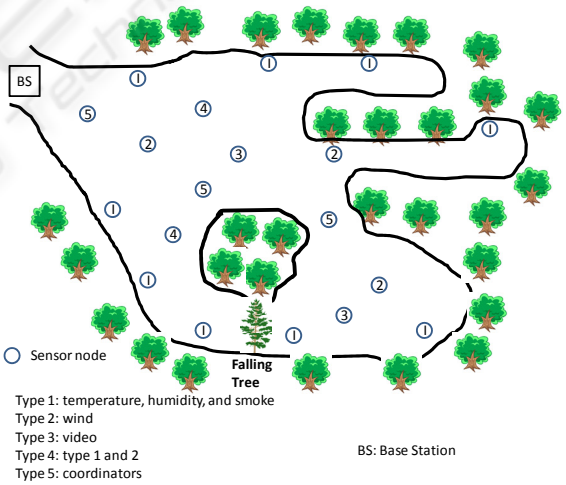

Figure 1: A forest fire-monitoring WSN application.

3 SECURITY CHALLENGES

Security (Djenouri, Khelladi and Badache, 2005; Wang, Attebury and Ramamurthy, 2006; Walters, Liang, Shi and Chaudhary, 2006) is a key factor in protecting sensitive applications and data communications. Challenges arise as emerging applications evolve to support mobility, required in

more dynamic environments. Mobility in WSNs creates a new security paradigm as communication patterns are dynamically formed and therefore investigations must be made to identify ways in which security is affected in such dynamic environments. Currently, one of the biggest concerns is that existing security mechanisms in static WSNs may not be capable of supporting security requirements in dynamic mobile environments. Therefore, we need to investigate if existing security mechanisms can be applied/adopted to the new application paradigm and also if new security challenges dictate the creation of new security mechanisms.

Connectivity is one of the most important attributes that mobile sensor nodes must establish to support network communication. In this paper we investigate the routing operation (Akyildiz, Su, Sankarasubramaniam, Cayirci, 2002; Al-Karaki and Kamal, 2004) as it is one of the fundamental operations in WSNs that facilitates the establishment of communication links between sensor nodes and packet delivery. Securing the routing operation involves two main aspects: (i) protecting the confidentiality and integrity of the control and data packets that are routed to the intended destination, and (ii) establishing routing paths to the destination in a way that promotes a highly available and reliable environment. For each aspect, an appropriate security area can be considered and supports specific security requirements (Carman, Kruus and Matt, 2000; Wang, Attebury and Ramamurthy, 2006; Walters, Liang, Shi and Chaudhary, 2006). The main security requirements in a mobile environment are: (i) network reliability, availability, and resiliency; (ii) authentication of nodes; (iii) data integrity; and (iv) data confidentiality.

These requirements are provided through a number of functionalities that introduce security in the network. Key management schemes can be used to establish security associations (SAs) between communicating parties and protect the routing path establishment procedures and the data forwarding operations against attacks launched by malicious nodes. Trust management schemes can be used to aid sensors to select the next-hop node based on its reputation. Multipath routing support can enhance the packet reliability (Ganesan, Govindan, Shenker and Estrin 2002; Ye, Zhong, Lu, Zhang 2005). All the aforementioned security areas have been substantially investigated in fixed WSN environments. However, security issues and challenges in mobile WSNs have not been given much attention. Next, we briefly analyze the approach taken in each security area and then identify the security challenges raised due to the nodes' mobility.

3.1 Key Management

Authentication is required prior to the deployment of any security mechanism as it facilitates the establishment of SAs. SAs imply some level of trust among nodes as partners verify each other's identity. A Key Management System (KMS) creates, distributes, and manages these identification credentials used in the establishment of SAs. The challenges with key management increase in future sensor networks since sensor nodes do not only have limited battery power and computation capability but they now require more complicated and dynamic SA establishments. Furthermore, solutions need to be able to address scalability as future sensor networks will be comprised of thousands of sensor nodes.

Key management in sensor networks typically uses Key encryption keys (KEKs) that are in turn used to (re-)distribute session keys and secure communication among nodes by establishing SAs. Mobility of sensor nodes requires that session keys be changed more frequently to assure resilience against attacks and to accommodate changes in the characteristics of the networks, such as topology, number of nodes, and their individual role (e.g., cluster head).

In the near future, we envision that sensor nodes will continue to use symmetric keys since they have lower computational requirements than asymmetric keys. It may still, however, be helpful to harness some of the benefits of asymmetric cryptography (such as lower key distribution overhead) to initialize the configuration of symmetric keys on the nodes. At present the overhead of calculating an ECC point multiplication for public key cryptography in a sensor device is not high [Aranha, Oliveira, Lopez, and Dahab, 2009.]. Previous analysis of static scenarios assumed that the connectivity patterns are limited from source to BS. In our aforementioned scenario we require more complicated communication patterns, which may imply a relatively larger number of SAs. Even though research in (Mizanur Rahman, Nasser and Saleh, 2008) focused on minimizing the generation of keys based on the traffic patterns in the network, they did not take into account the existence of large sensor networks. Scalability issues need to be addressed more aggressively. It is also important to mention that if nodes utilize symmetric keys then the management complexity increases towards a

maximum n(n-1)/2 keys, when shifting towards a mesh type of connectivity in terms of SAs (i.e., all the nodes in the network trust one another).

Previous solutions in the literature that utilized a network wide symmetric key for all the nodes no longer constitute solutions for key management. Even if the network-wide symmetric key is used to establish new keys per pair this strategy leads to problems with synchronization during periodic updates of keys in the face of mobility. Furthermore, solutions that suggest the deletion of the network-wide key for added security do not generally work as they imply the existence of a closed system that does not accept new sensor nodes.

Another aspect that has not been taken into account is the trustworthiness of a BS or the inference of the existence of SAs between the BS and all the sensor nodes. This approach does not scale and raises issues of security in terms of the BS being a centralized point of attack. One potential solution is to introduce multiple BSs in WSNs, but this has to be investigated carefully as multiple BSs increase the complexity in terms of data flow directions and introduce extra key management overhead (the relationship between SAs and BSs becomes many-to-many).

A common approach for key management is through the use of a random key pre-distribution protocol (Eschenauer and Gligor, 2002;Chan, Perrig and Song, 2003; Liu and Ning, 2005; Liu, Ning and Du, 2005; Guorui, Jingsha and Yingfang, 2006; Ting, Shiyong and Yiping, 2007). (An investigation of the resilience of key management for random key pre-distribution is offered in (Yulong, Jianfeng and Qingqi, 2007)). Each node has a subset of symmetric keys that is randomly selected from a large pool of keys and communicates with nodes that have a similar key pool. The limitation of these KMSs is that they do not dynamically adjust to accommodate new nodes or changing environment conditions in the network, such as battery limitations, heterogeneous nodes, topology changes, or coverage area changes. Thus, it is difficult to establish the required number of SAs by discovering common keys. Moreover, an attacker, can take advantage of mobility and more easily compromise enough nodes to obtain a large number of symmetric keys and thus break the security of the system. The authors in (Liu, Ning and Du, 2005) and (Du, Deng, Han, Chen Sand and Varshney, 2004) have alleviated the limitation of building SAs in a changing environment by ensuring that nodes that are closer together have more common keys. This solution took advantage of pre-deployment knowledge prior to the network deployment. However, this assumption does not fully accommodate the scenario of mobile sensors and dynamically changing sensing areas, such as in the case of a falling tree (see Figure 1). A promising solution that avoids pre-deployment knowledge of sensor nodes and accommodates an open system was proposed by Anjum (2007). He proposed a scheme that utilized anchor nodes with higher radio range, which execute location dependent key management. Even though this solution might be applicable to future sensor networks it requires careful deployment of anchor nodes, which makes it less flexible. In addition, it needs to be augmented to take care of certain limitations. More specifically, nodes that are inserted start with the same initial network key and the anchor nodes transmit the same nonces for key negotiations. This feature prevents any network-wide rekeying of the sensor nodes, which makes the network more vulnerable to attacks. The anchor nodes would also need to be made mobile and their movements would need to be carefully selected to provide full coverage of the network and maximize the availability of the key management service in the WSN. Thus, the scenario in Figure 1 would need to take into account a hybrid network of mobile ad hoc (represented by the anchor nodes) and sensor networks, where one network helps with the deployment of the other one. A new hybrid KMS solution must be designed that will accommodate a higher key management complexity.

Another aspect that would need more investigation with regards to key management is energy in light of nodes that utilize the active/sleep state (Riaz, Ali, Kim, Ahmad and Suguri, 2006). Such a scheme can not apply in our scenario as it assumes the existence of densely deployed WSNs, which may not necessarily be the case in the future since mobility may be used to provide full coverage of a dynamically changing environment. Furthermore, this methodology creates complications for key management for cases where nodes are allowed to enter sleep mode. In addition, this scheme needs to be augmented as it suffers from the design of having one non-changing initial network/global key.

A challenge that has not been given a lot of attention in sensor networks with regards to key management is revocation. A centralized solution for revocation is not applicable as the BS that broadcasts such revocations needs to be able to communicate with all the mobile sensor nodes. In addition, it is not clear how the BS will acquire the information, such as bad behaviour, required to guide revocation decisions. Thus, such a solution is

not feasible. A distributed revocation scheme has been proposed in (Eschenauer and Gligor, 2002) and enables the neighbours of a compromised node to revoke it. This approach still suffers from the limitations of broadcast communication, which makes it slower in terms of response and increases the overhead in the network as all the nodes need to remember the grading of their peers. Furthermore, it is not clear how this grading can be amended when mistakenly taking a node to be malicious. An effective revocation needs to be more responsive, execute localized revocation, and be flexible in terms of its assessments. This needs to allow for the remuneration of a node's reputation when its behaviour is improving and for harsher measures if its behaviour switches to very bad. Basically, this approach needs to take into account a node's cooperation over time. This is a topic that has been investigated in more depth through social networking and game theory. It is important to note that the authors in (Chan, Gligor, Perrig and Muralidharan, 2005) have investigated revocation within time bounds to address the notion of stale votes that may lead to erroneous revocation of nodes. They used hop-limited local broadcast of reputation information nodes but allowed only one network-wide broadcast when the final revocation decision is taken. Thus, the network overhead was kept at a minimum and communication was successful assuming there was connectivity. These solutions form a good basis for revocation, but need to be extended to accommodate more dynamic scenarios where mobility coupled with energy constraints introduces new challenges.

Summarizing, key management should be carefully studied in the context of future networks as it lies at the heart of the network defences. To support secure routing, key management will need to supply the necessary keys to enable point-to-point, point-to-cluster, intra-cluster communication, etc. These modes of communication must be supported to a large scale and in multiple directions between the network nodes. This is a paradigm that is different compared to existing sensor networks. Inferring pre-deployment knowledge and random key pre-distribution to aid key management is not always feasible as the area of coverage change and nodes move in different direction. Other aspects that need careful study are revocation and the impact of key management on energy schemes or the reverse (i.e., how energy schemes affect the operation of the key management system).

3.2 Multipath Routing Support

In mission-critical applications, what values the most is observation data that indicates if a critical event has occurred. Therefore, establishing network reliability and resiliency can support the timely detection of critical events and decision making. A reliable and resilient routing operation means that the data is delivered to the intended destination, even in the face of attacks. The common practice in resource-constrained WSNs is to deploy single path routing. Approaches in multipath routing apply to single path routing; thus, we only focus on multipath routing in our investigation. Generally, failure of nodes along the path would mean failure of the path and loss of data. This is unacceptable in mission-critical applications that rely on the timely delivery of observations to support application objectives. Currently, a number of WSN-based multipath routing protocols integrated with security mechanisms have been proposed in the literature (Deng, Han and Mishra, 2002; Lou and Kwon, 2006; Ouadjaout, Challal, Lasla and Bagaa, 2008; Stavrou and Pitsillides, 2010; Ma, Xing and Michel, 2007), considering fixed sensor nodes. In these protocols, a source node discovers its neighbouring nodes and deploys multipath routing to forward packets to the intended destination, supporting a reliable and resilient environment.

In a mobile WSN environment, a number of challenges are raised regarding multipath routing:

a) Routing does not converge to a stable state due to frequent node movements. The main concern is that the route discovery process needs to be initiated frequently to discover new routes to the destination.

b) Multipath routing is by default a costly operation in terms of communication and energy consumption. Mobility further increases a node's energy consumption and so does the usage of cryptographic mechanisms by the routing protocol due to the frequent updates. Furthermore, end-to-end versus hop-to-hop security should be considered in the routing protocol design in order to minimize the SAs established between sensor nodes and the usage of cryptographic algorithms, and conserve nodes' resources. In addition, mobile routing protocols in WSNs should be designed such that mobile nodes provide different multipath levels (in terms of the path number) based on the packet content in order to balance the required packet reliability e.g., handle differently smoke data and temperature data in our scenario.

c) Moving nodes contributing in multipath routing do not know their surrounding nodes and therefore

do not know which nodes to trust for collaboration. The challenge here is to distinguish between trusted and untrusted nodes in order to forward packets through trusted nodes and increase the possibility for a successful packet delivery. Trust management is treated in the following subsection.

3.3 Reputation - based Trust Management

Reputation-based trust schemes, add another layer of security that goes beyond the capabilities of the utilized cryptographic mechanisms. The idea is to evaluate the behaviour of nodes over time in order to guide collaboration in the network. For example, sensor nodes may decide which paths to use based on the reputation ratings of their peers.

Reputation metrics may involve the capability of correct packet forwarding of sensors, intrusion detection results, recommendations from neighbour nodes, etc. A number of reputation-based trust schemes have been proposed in the literature. For example, (Marti, Giuli, Lai and Baker, 2000) proposed a reputation-based scheme composed of a watchdog and a pathrater module in order to determine if intermediate nodes are indeed forwarding the received packets. The watchdog node overhears the communication to verify whether its neighbouring node has forwarded the packet. Based on the result, the pathrater rates each path and chooses a path to avoid misbehaving nodes. The concept of monitoring and rating forms the basic functionality of a reputation trust-based framework that is applied according to the aspects that need to be evaluated. In (Tanachaiwiwat, Dave, Bhindwale and Helmy, 2003; Yao, Kim, Lee, Kim and Jang, 2005) authors define reputation metrics related to cryptographic operation, availability of nodes to provide service, and nodes behaviour that can indicate malicious activity. In (Crosby, Pissinou and Gadze, 2006), authors follow a similar trust evaluation approach to aid the election of trustworthy cluster heads. Another approach is taken by (Liu, Abu-Ghazaleh and Kang, 2007) where they not only favour well behaving nodes for each successful packet forwarding, but also penalize suspicious nodes that lie about their contribution to routing.

The existing trust management schemes cannot be fully applied in mobile WSNs application because due to mobility it is difficult to monitor the behaviour of mobile nodes in order to compute their reputation value. The idea of partitioning the network in clusters such as in (Crosby, Pissinou, Gadze and 2006) aids trust management by allowing cluster nodes to check for malicious behaviour and verify falsified information. Clustering has been promoted due to its energy saving capabilities within the network. However, clustering cannot always exist in future scenarios due to mobility, and due to the fact that changes in the sensing area may require that clusters be reformed dynamically. Thus, the underlying difficulty in terms of mobile sensors is to designate monitoring nodes in a mobile environment such that they can effectively record the behaviour of all the nodes in the network. In addition, the reputation metrics of a mobile node need to be globally trusted so that if it needs to cooperate with other nodes while moving around its reputation will be trusted by its peers. The trust management scheme should provide different trust levels such as in (Yao, Kim, Lee, Kim, Jang, 2005), but at the same time create semantics for the various trust levels so that they can match specific functionalities within the networks. For example, different levels of trust may indicate authorization to forward a packet or authorization to accept sensing observations for a particular metric. Also, for the case where packets need to be forwarded through nodes with low reputation values (due to lack of trusted nodes), there needs to be integration with security mechanisms such that security enhancements are utilized. Reputation-based trust management schemes can be very useful, but the trade-off between reliability, compromization risk, and performance needs to be balanced.

4 SECURITY AND ENERGY EFFICIENCY

Energy is the most important resource in WSNs due to the limited resources of sensor nodes (Akyildiz, Su, Sankarasubramaniam and Cayirci, 2002). Usually, sensor nodes use batteries as their main energy source and it is not always feasible to replace them when depleted. There are several sources of energy consumption in sensor networks, such as when communicating, sensing and processing information, with the former being the most energy demanding operation. By adding extra functionality in a sensor network, it further contributes to the overall energy consumption. A potential energy depletion of some of the sensor nodes can greatly affect the survivability of the network, since it can cause the degradation of the routing operation. This depletion can eventually lead to network partitions

prohibiting observations on a specific area and affecting the successful operation of the application. The challenge is even greater when mobility is introduced in the network. Mobile nodes require energy to be able to move. The amount of energy being consumed is dependent on the movement frequency and the distance that sensor nodes have to cover.

In terms of key management, a mobile node has to establish SAs with other nodes along the motion path. This task requires extra energy due to the communication and processing required, that is dependent on the number of SAs that need to be negotiated and established. The challenge for mobile nodes is to establish the minimum required number of SAs that utilize cryptographic schemes for secure communication taking into account paths that change dynamically, and still supporting an acceptable security level, adequate to protect the network environment.

In terms of supporting reliable and resilient routing, multipath routing is typically recommended to be deployed. However, in multipath routing, more than one path is established to forward a packet from source to destination. This redundancy means that communication overhead is increased as the number of alternative paths increases, leading to extra energy consumption. Node mobility leads to a dynamic environment, where communication links change according to nodes motion. Since mobile nodes are not aware of their surrounding environment, they have to re-initiate the route discovery procedure in order to discover different routes to the destination. This is a costly operation in terms of energy consumption that greatly affects the lifetime of mobile sensor nodes.

In terms of trust management, node mobility leads to uncertainty about trust in the surrounding environment. Reputation-based information should be requested from other nodes/entities to aid mobile nodes decide which nodes to trust and use for forwarding packets. This uncertainty about trust also applies in the opposite direction. That is, when a mobile node moves to a new area and requests to establish communication with a neighbouring node, that neighbouring node is not certain about the mobile node's trustworthiness. It has to request reputation-based information from another entity. All these actions to support trust management in a mobile environment require again extra communication between sensor nodes, which lead to increased energy consumption.

A trade-off between security and energy efficiency in mobile WSNs can only be achieved if we have a clear understanding of the environment and the application's security needs and objectives. It is clear that mobile sensor nodes consume much more energy than static nodes. Therefore, to promote the survivability of the network, nodes with heterogeneous resources should be considered. Investigations should focus on how heterogeneity can aid sensors mobility and permit the implementation of resource-aware security mechanisms.

5 CONCLUSIONS

This paper investigated security issues and challenges in next generation mobile sensor networks. State of the art in security in sensor networks has focused on fixed sensor networks with pre-defined communication patterns over fixed areas. We argued that changing deployment areas, heterogeneous sensors, and dynamic communication patterns driven by mobility and varying sensing requirements would be required in next generation sensor networks. We have presented a realistic fire scenario with multiple sensors that motivated such a future direction. Based on our investigation with regards to key management, routing, trust management, and energy, we identified issues that reveal the inflexibility of systems and functionalities due to the inherent built-in assumptions about the environment, the nodes, their roles, the data, and the communication patterns. It is clear that we need solutions that can be dynamically adjusted based on the requirements of the data flows that may depend on the communication of heterogeneous sensor nodes, which may have varying roles in the network. In addition, these solutions will need to be robust in the face of mobility, energy limitations, and changing or unknown coverage areas.

ACKNOWLEGEMENTS

This research work is supported by ASPIDA (KINHT/0506/03) and by the TRUST project, funded by Cyprus Research Promotion Foundation (ΤΠΕ/ΠΛΗΡΟ/0308(ΒΕ)/10).

REFERENCES

Akyildiz I. F., Su W., Sankarasubramaniam Y. and Cayirci E., (2002), Wireless Sensor Networks: A Survey,

Computer Networks, *Elsevier Journal*, 38(4), 393-422.

Al-Karaki, J. N. and Kamal, A. E., (2004). Routing techniques in wireless sensor networks: a survey, *IEEE Wireless Communications*, 11(6), 6-28.

Anjum F. (2007). Location dependent key management in sensor networks without using deployment knowledge. *2nd International Conference on Communication Systems Software and Middleware*, 1-10.

Aranha D., Oliveira L. B., Lopez J., Dahab R. (2009). *NanoPBC: Implementing Cryptographic Pairings on an 8-bit Platform*. CHILE.

Carman D. W., Kruus P. S. and Matt B. J., (2000). Constraints and approaches for distributed sensor network security, *NAI Labs Technical Report* #00-010

Chan, H., Perrig, A., 2003, Security and Privacy in Sensor Networks, *IEEE Computer Magazine*, pp. 103-105

Chan H., Perrig A. and Song, D. (2003). Random Key Predistribution Schemes for Sensor Networks. *IEEE Security and Privacy Symposium*, 197–213.

Chan H., Gligor V.D., Perrig A. and Muralidharan G., (2005 July-September). On the distribution and revocation of cryptographic keys in sensor networks. *IEEE Transactions on Dependable and Secure Computing*, 2(3), 233- 247.

Crosby G. V., Pissinou N. and Gadze J. (2006). A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks, *Proceedings of the Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems*

Deng J., Han R. and Mishra S., (2002). INSENS: Intrusion-Tolerant Routing in *Wireless Sensor Networks, Technical Report* CUCS-939-02, Department of Computer Science, University of Colorado

Djenouri, D., Khelladi, L., Badache, A.N., (2005). A survey of security issues in mobile ad hoc and sensor networks, *IEEE Communications Surveys & Tutorials*, 7(4), 2- 28.

Du W., Deng J., Han Y S., Chen Sand Varshney, P. K. (2004 April). A key management scheme for wireless sensor networks using deployment knowledge. *INFOCOM*.

Eschenauer L. and Gligor V. (2002 November). A Key Management Scheme for Distributed Sensor Networks. *9th ACM Conference. Computer. and Communications Security*, 41-47.

Ganesan D., Govindan R., Shenker S. and Estrin D., (2002). Highly-Resilient Energy-Efficient Multipath Routing in Wireless Sensor Networks, ACM Mobile *Computing and Communication Review* (MC2R), 1(2).

Garcia-Hernandez C. F., Ibarguengoytia-Gonzalez P. H., Garcia-Hernandez J. and Perez-Diaz J. A. (2007). Wireless sensor networks and application: a survey, *International Journal of Computer Science and Network Security (IJCSNS)*, 7(3).

Guorui L., Jingsha H. and Yingfang F. (2006). A hexagon-based key predistribution scheme in sensor networks. International *Conference on Parallel Processing Workshops*, 180.

Karlof C. and Wagner D. (2003). Secure routing in wireless sensor networks: Attacks and Countermeasures, *IEEE International Workshop on Sensor Network Protocols and Applications*, 113-127.

Liu K., Abu-Ghazaleh N. and Kang K. (2007). Location verification and trust management for resilient geographic routing, Location verification and trust management for resilient geographic routing, 67(2), 215-228.

Liu D., Ning P. and Du W. (2005, September). Group-Based Key Pre-Distribution in Wireless Sensor Networks. *ACM Workshop on Wireless Security (WiSe)*, 11–20.

Liu D. and Ning P. (2005). Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks. *ACM Trans. Sensor Networks*, 204–39.

Lou W., Kwon Y., (2006). H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. *IEEE Transactions on Vehicular Technology*, 55(4), 1320 – 1330.

Mizanur Rahman Sk. Md., Nasser N. and Saleh K. (2008). Identity and Pairing- Based Secure Key Management Scheme for Heterogeneous Sensor Networks. *IEEE International Conference on Wireless and Mobile Computing, Networking and Communication*, 423-428.

Ma R., Xing L. and Michel H. E., (2007, May). A New Mechanism for Achieving Secure and Reliable Data Transmission in Wireless Sensor Networks. *The 2007 IEEE Conference on Technologies for Homeland Security*, 274-279.

Marti S., Giuli T., Lai K., and Baker M., (2000). Mitigating routing misbehavior in mobile ad hoc networks, *In Proceedings of MOBICOM*

Ouadjaout A., Challal Y., Lasla N. andBagaa, M., (2008 March) SEIF: Secure and Efficient Intrusion-Fault Tolerant Routing Protocol for Wireless Sensor Networks, *Third International Conference on Availability, Reliability and Security (ARES)*, 503-508.

Riaz R., Ali A. Kim K. Ahmad H. F. and Suguri, H, (2006). *Secure Dynamic Key Management for Sensor Networks. Innovations in Information Technology*, 1-5.

Stavrou E., Pitsillides A., (2010), A survey on secure multipath routing protocols in WSNs, accepted for publication, Computer Networks, *Elsevier Journal*, http://www.netrl.cs.ucy.ac.cy/index.php?option=com_jombib&Itemid=60

Tanachaiwiwat S., Dave P., Bhindwale R., Helmy A., (2003). Secure Locations: Routing on Trust and Isolating Compromised Sensors in Location-aware Sensor Networks. *The First ACM Conference on Embedded Networked Sensor Systems (SenSys)*.

Ting Y.,Shiyong Z. and Yiping Z. (2007). A Matrix-Based Random Key Predistribution Scheme for Wireless Sensor Networks. *IEEE International Conference on Computer and Information Technology*, 991-996.

Walters J. P., Liang Z., Shi W. and Chaudhary V., (2006). Wireless Sensor Networks Security: A Survey, Security *In Distributed, Grid and Pervasive Computing*, CRC Press

Wang Y., Attebury G. and Ramamurthy B. (2006). A survey of security issues in wireless sensor networks, *IEEE Communications Surveys & Tutorials*, 8, (2), 2 – 23.

Wood A. D. and Stankovic J. A., (2002). Denial of Service in Sensor Networks, *IEEE Computer*, 35(10), 54-62.

Wood A. D. and Stankovic J. A. (2004). A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, *CRC Press*

Ye F., Zhong G., Lu S. and Zhang L.,(2005). GRAdient broadcast: A robust data delivery protocol for large scale sensor networks, In *ACM Wireless Networks (WINET)*, 11(2).

Yao Z., Kim D., Lee I., Kim K. and Jang J., (2005). A Security Framework with Trust Management for Sensor Networks, *Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*,190-198.

Yulong S., Jianfeng M. and Qingqi P. (2007). Research on the Resilience of Key Management in Sensor Networks. *International Conference on Computational Intelligence and Security*,716-720.