I J C T A, 9(2) 2016, pp. 903-910

Novel Key Management Techniques in Three-Tier Wireless Sensor Networks

[1]A. Senthil Kumar and [2]E. Logashanmugam

ABSTRACT

The Three Tier Security Scheme for Wireless Sensor Networks (WSNs) was introduced basically to improve the cost efficiency of the system. This is because the incorporation of asymmetric keys increases the computational and memory costs. But, the cost of key pre distribution schemes is low and they provide secure communication between Sensor Nodes (SNs) and mobile sinks. However, Pair wise key establishment is not provided for guarantying security. Hence, we propose Novel Key Management Technique in Three Tier (NKM_TT) Wireless Sensor Networks to manage the security methods in a WSN. In this scheme, we use Message Authentication Code (MAC) to provide the data integrity. Digital signature grants authentication between the MS and AP as well as the Session Pairwise key provides authentication between AP and SN. Our analytical results indicate that the new security technique makes the network more resilient to both MS and stationary AP security and minimizes the computation cost compared to the polynomial pool-based approach.

Keywords: Message Authentication Code (MAC), Digital signature, Session Pairwise Key, Mobile Sink, Access Point, WSNs.

1. INTRODUCTION

Newest advances in electronic knowledge have covered the way for the growth of a new generation of wireless sensor networks (WSNs) consisting of a large number of small power and least cost SN that communicate wirelessly [1]. Sensor networks can be used in a wide range of applications, such as health monitoring data acquisition in hazardous environments, military sensing and tracking and habitat monitoring [2]. The sensed data often need to be sent back to the Base Station (BS) for investigation. However, while the sensing area is far away from the BS, transmitting the data over long distances using multihop may decline the security. Some intermediate may change the data passing by, capturing SNs, establishing a wormhole attack, a sybil attack, selective forwarding attack, sinkhole and rising the energy utilization at nodes near the BS, diluting the lifetime of the network. For that reason, MSs are necessary components in the function of many sensor network applications, including data gathering in harmful environments localized reprogramming, oceano-graphic data collection and military navigation. In many of these applications, SNs transmit significant information over the network; therefore, security services, for example, pairwise key establishment and authentication between SNs and MSs, are important. However, the resource constraints of the sensors and their nature of transmission over a wireless medium make data confidentiality and integrity a non-trivial duty.

To address the above-mentioned problem, we have developed a general three-tier security framework for integrity of transmitting data and authentication of AP and MS. The data integrity of this message is provided through MAC. The digital signature provides authentication between MS and AP. The use of a

[1] Research Scholar, Department of Electronics and Communication Engineering,
[1] St. Peter's University, Chennai, India
[2] Professor, and Head, Department of Electronics and Communication Engineering,
[2] Sathyabama University, Chennai, India

pairwise session key between the APs and SN guarantees the authentication. The proposed technique will significantly improve network flexibility to MS and AP security compared to the existing scheme.

The remaining of this paper is organized as follows: an overview of related works is described in section 2. Section 3 describes the Novel Key Management Technique for security solution. Section 4 provides the simulation analysis. Finally, we conclude our scheme in section 5.

2. RELATED WORKS

Statistical En-route Filtering (SEF) mechanism [3] detects the injected forged data in sensor network and mainly focuses on how to filter forged data using collective secret and thus prevents any single compromised node from breaking the entire system. TinySec [4] proposed a link layer security mechanism for sensor networks, which uses an efficient symmetric key encryption protocol. Dynamic Combinatorial Key Pre-distribution scheme (DCKP) [5] makes use of the Exclusion Basis System (EBS) and sensors location information. DCKP is very efficient in terms of storage at a certain local connectivity and provide better security. Secret instantiation in Ad hoc networks [6] analyzes the problem of assigning initial secrets to users in ad-hoc sensor networks to ensure authentication and privacy during their transmission and points out possible ways of sharing the secrets. Probabilistic secret sharing protocol [7] defends Hello flood attacks. This scheme uses a bidirectional confirmation technique and introduces multi-path multi base station routing if bidirectional confirmation is not adequate to defend the attack. Game-theoretical defense strategy [8] provides guaranteed high level of trustworthiness for sensed data. Trust and reputation systems [9] play critical role in WSNs as a method of resolving a number of important problems, for example secure routing, false data detection, fault tolerance, secure data aggregation, cluster head election, compromised node detection, outlier detection, etc.

Packet dropping and modification are common attacks [10] that can be launched by an adversary to interrupt transmission in wireless multi hop sensor networks. This scheme is used to catch both packet droppers and modifiers. While the tree formation vigorously changes every time period, behaviors of SNs can be observed in a large variety of scenarios. The information of node behaviors can be used to identify bad nodes from suspiciously bad nodes. Secure and reliable data aggregation [11] assures security and reliability of aggregated data in the presence of compromised sensor nodes. The trust development algorithm is used to ensure the reliability of aggregated data and to select secure and reliable paths. Hashed Random Key Pre-distribution Scheme [12] provides secure connectivity and scalability. It utilizes hashed random key pre-distribution scheme for large sensor networks that realize authentication of pool keys and broadcast messages of auxiliary nodes. This security scheme limits attack range of node compromise and that hash chains have good properties to protect the phases of key revocation and addition of new sensor nodes.

3. PROPOSED METHOD

The sensor node has limited energy and storage capabilities and it has become a primary challenge to provide security functions. The Enhanced Three Tier security scheme (E-TT) was robust against a stationary Access node replication attack, as this scheme makes use of a one-way hash chains algorithm along with the static polynomial pool based scheme [13]. However, this scheme suffers from many drawbacks. It is very difficult to know the correct number of polynomials required for having a connection. The main problem with this is the communication overhead as a result of this it takes a considerable amount of time. Therefore, to overcome this problem, we have introduced a Novel Key Management Techniques in Three Tier Wireless sensor networks (NKM-TT). This Novel key provides security between the access nodes and the mobile sinks as well as sensor node and access node communication.

In this scheme, Message Authentication Code (MAC) provides data integrity and we use digital signature to offer authentication among MS and AP as well as pairwise session key provide security between AP and SN. This minimizes the computation cost and provides the secure data transmission from SN to MS.

This system contains number of pre selected sensor nodes called the stationary Access Node which acts as Access points (APs) in the network. Mobile Sink (MS) send data request message to the Sensor Nodes (SNs) through the APs. This APs triggers the SNs that transmits their data to the MS. Pairwise Session keys are generated between the MS and AP as well as AP and SN. Figure 1 illustrates the example of Three Tier Architecture.

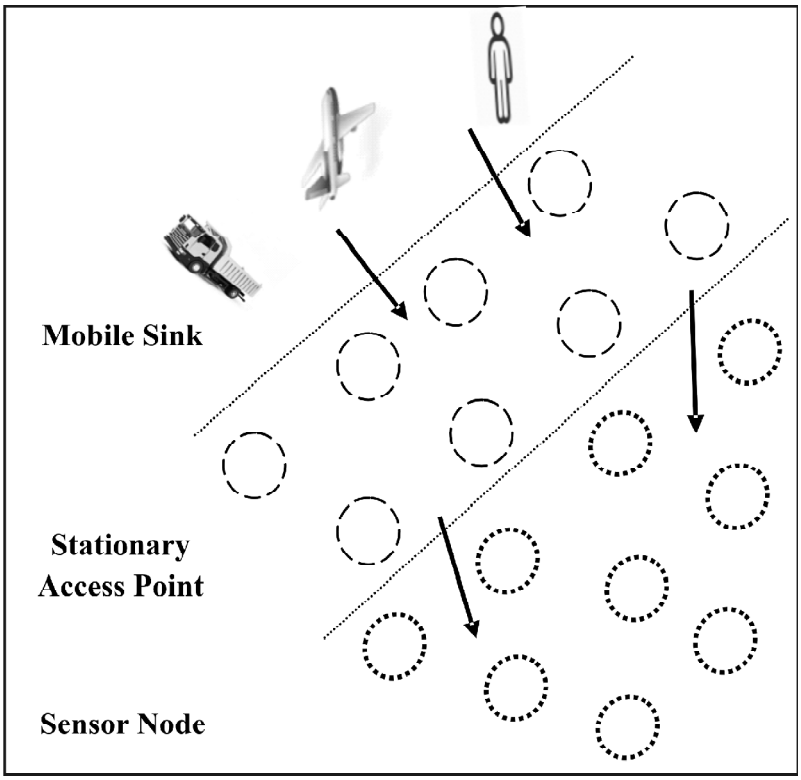

Figure 1: Three-Tier Architecture

MS send Data Request DREQ message to the AP. This message contains AP id and MS id and its signature.

$$MS \rightarrow AP \Rightarrow id_{MS}, id_{AP}, sig_{MS}(id_{MS}, id_{AP}) \tag{1}$$

AP receives this message and verifies the MS signature. The session key is calculated as $K_{AP} = hash(K_{AP})$, SN also contain the same key.

Then AP broadcast Join request (JREQ) message to the SNs. SN and AP share the pairwise session key $K_{SP} = hash(K_{SP} \| t_{st})$.

$$AP \rightarrow SN \Rightarrow id_{AP}, id_{SN}, t_{AP}, K_{SP} \tag{2}$$

SN checks pairwise session key. If the key matches then SN send JRREP (Join Reply) message to the AP.

$$SN \rightarrow AP \Rightarrow id_{SN}, id_{AP}, K_{SP} \tag{3}$$

AP checks the pairwise session key. If the key matches then AP send RREP (Route Reply) message to the MS.

$$AP \rightarrow MS \Rightarrow id_{AP}, id_{SN}, sig(id_{AP}, id_{SN}) \tag{4}$$

MS verifies the authenticated AP and obtain the valid route.

Finally, the SN sends encrypted data to the valid route via authenticated AP. MAC computation provides the security for data transmission.

$$SN \rightarrow AP \Rightarrow id_{AP}, id_{SN}, enc_{k_{SN}}(d_{SN}), mac_{K_{SP}}(id_{SN} \,||\, id_{AP} \,||\, enc_{K_{SN}}(d_{SN})) \quad (5)$$

The authenticated AP sends the data to MS

$$AP \rightarrow MS \Rightarrow id_{AP}, id_{MS}, enc_{k_{SN}}(d_{SN}), mac_{K_{AP}}(id_{AP} \,||\, id_{MS} \,||\, enc_{K_{SN}}(d_{SN})) \quad (6)$$

Where

$id_{SN} \rightarrow$Sensor Node id

$id_{AP} \rightarrow$Access Point id

$D_{SN} \rightarrow$Sensor Data

$K_{SP} \rightarrow$Pairwise Session Key

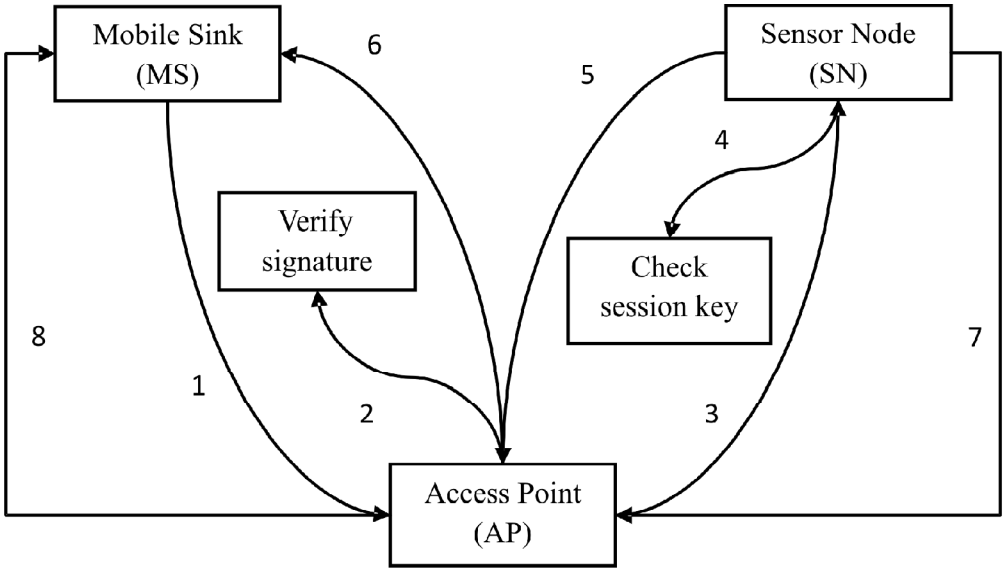

Figure 2: Working Flow of Proposed Scheme

Figure2 shows the working flow of the proposed scheme. This detail explanation steps are given below.

Step 1: Initially the MS wants to collect the data from particular SN. Hence, MS send data request to the AP.

Step 2: The AP verifies the signature of the MS.

Step 3: If the signature is valid then the AP send the join request message to the SN.

Step 4: The SN checks the pairwise session key.

Step 5: If the pairwise session key matches, then the SN sends the JRREP message to the AP.

Step 6: Then the AP send RREP message to the MS.

Step 7: The SN send encrypted data to the AP. MAC computation checks the integrity of data.

Step 8: The AP collect the data from the SN and send this data to authenticated MS.

4. PERFORMANCE EVALUATION

The performance of the existing system E_TT is compared with the proposed NKM_TT system, which is presented in this paper using simulation results. A scenario of 50 nodes is randomly deployed in an area of 1000x1000m as shown in the table 1. In order to analyze the performances, the packet delivery rate, packet loss rate, delay rate and throughput are compared through simulations.

Table 1
Simulation parameters

Parameter	*Value*
Simulation Time	30s
Number of Nodes	50
Routing Protocol	E_TT and NKM_TT
Traffic Model	CBR
Simulation Area	1000x1000
Transmission Range	250
Antenna Type	Omni Antenna
Network Interface Type	WirelessPHY
Channel Type	Wireless Channel

4.1. Packet Delivery Rate

The Packet delivery rate is the ratio of the total packets delivered by the senders to the corresponding receivers in the network. It is given by the equation 7, where n represent the number of nodes in the network.

$$PDR = \frac{\sum_0^n PktsReceived}{time} \tag{7}$$

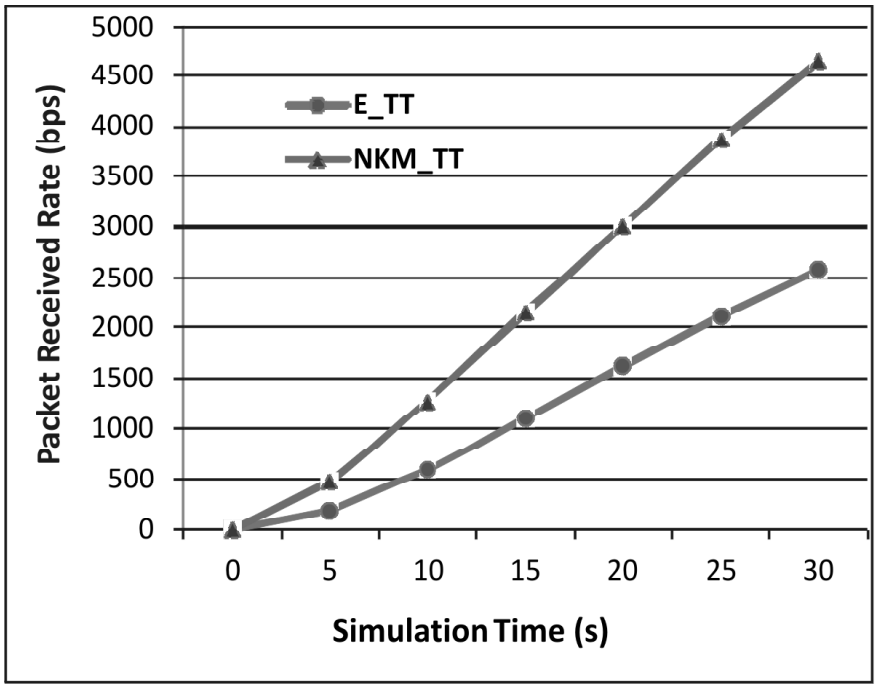

Figure 3: Packet Received Rate

The figure 3 shows the PDR of the proposed scheme NKM_TTS is higher than the PDR of the existing method E_TTS.

4.2. Packet Loss Rate

Packet Loss Rate is the ratio of the packets lost while senders send their packets to their corresponding receivers. It is given by the equation 8, where n represent the number of nodes in the network.

$$PLR = \frac{\sum_0^n PktsLost}{time} \tag{8}$$

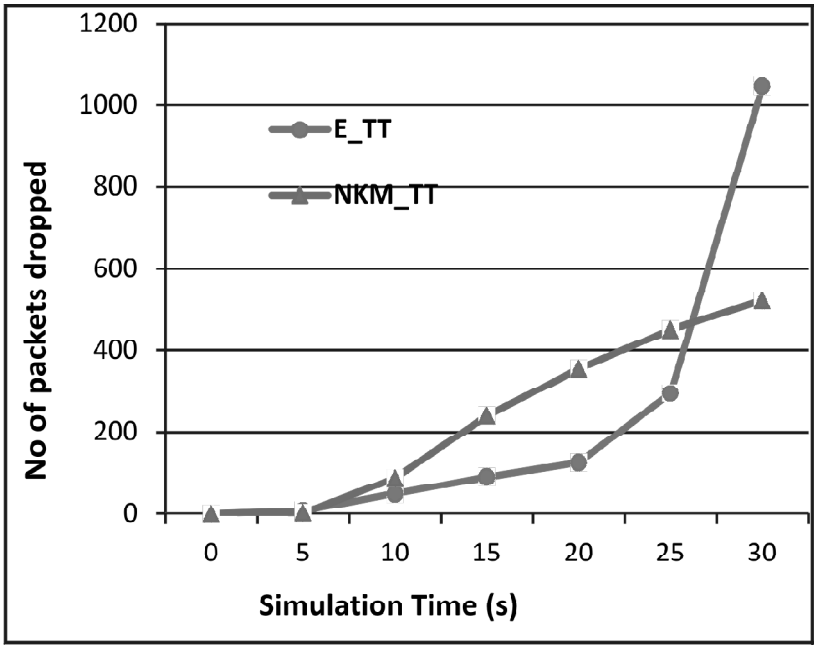

Figure 4: Packet Loss Rate

Figure 4 shows that the total packets lost of E_TTS are greater when compared to the NKM_TTS mechanism. The NKM_TTS has reduced packets lost due to highest security routing.

4.3. Delay

Average Delay refers to the time difference between packets sent and packets received. It is given by the equation 9, where n represent the number of nodes in the network.

$$Delay = \frac{\sum_0^n (PktRecvTime - PktSentTime)}{n} \tag{9}$$

The average delay is plotted in figure 5, which shows that the delay value is low for the proposed scheme NKM_TTS than the existing scheme E_TTS. The minimum value of delay means that higher value of the throughput of the network.

4.4. Throughput

Throughput is the total number of packets received by the receivers successfully. The average throughput is estimated using equation 10, where n represent the number of nodes in the network.

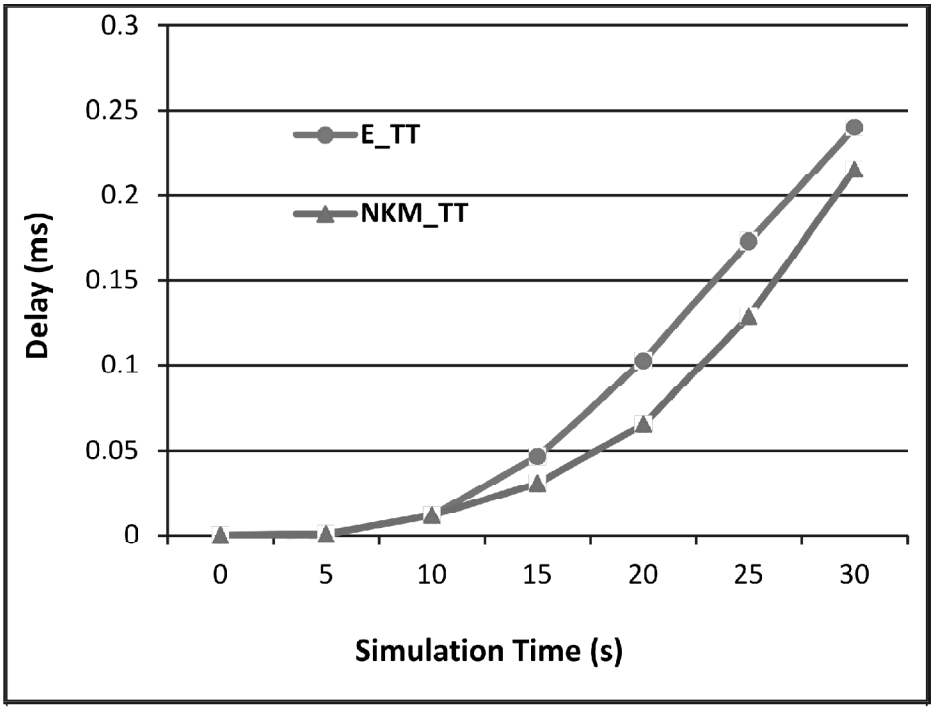

Figure 5: Average Delay

$$Throughput = \frac{\sum_0^n Pkts\ Received\ (n) * Pkt\ Size}{1000} \tag{10}$$

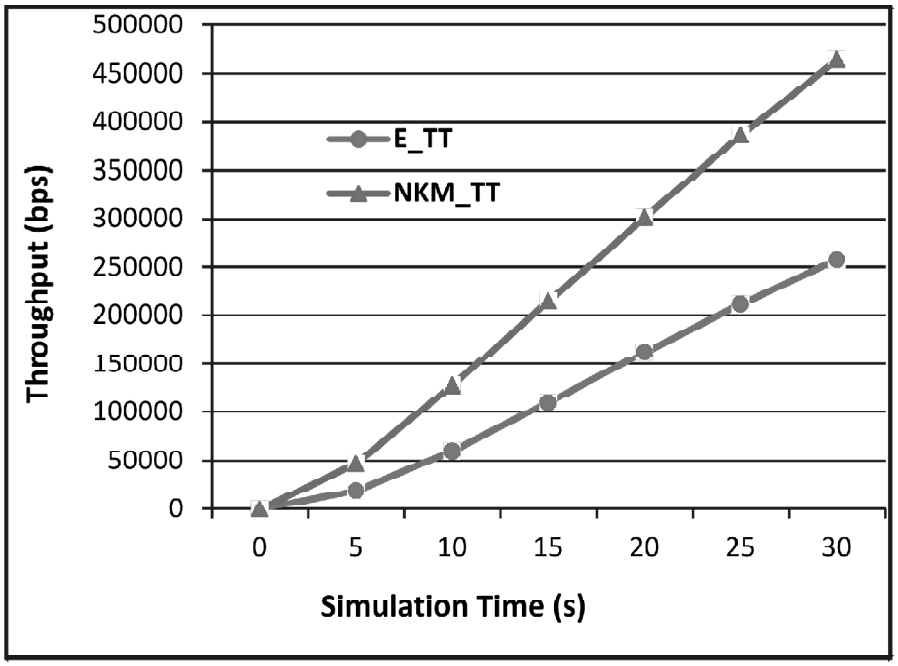

Figure 6: Throughput

Figure 6 show that NKM_TTS has greater average throughput when compared to the E_TTS mechanism. The security activity has improved the network performance greatly.

CONCLUSION

In this paper, we proposed a Novel Novel Key Management Techniques in Three Tier Wireless sensor networks to provide integrity, confidentiality and authentication. Before the transmission of data, digital signature checks the authenticated Mobile Sink and Pairwise Session Key checks the Access Point for verification. Message Authentication Code (MAC) checks the integrity of data for data transmission from Mobile Sink to Sensor Node. This security technique makes the network more resilient to both mobile sink and stationary access nodes and minimizes the computation cost compared to the polynomial pool-based approach. The simulation results demonstrate that the proposed scheme increase the throughput and reduce both the packet loss and delay of the network.

REFERENCES

[1] Yang, Qiuwei, *et al*. "Survey of Security Technologies on Wireless Sensor Networks." Journal of Sensors (2015).

[2] T. Gao, D. Greenspan, M. Welesh, R.R. Juang, and A. Alm, "Vital Signs Monitoring and Patient Tracking over a Wireless Network," Proc. IEEE27th Ann. Int'l Conf. Eng. Medicine and Biology Soc.

[3] Ye, F., Luo, H., Lu, S, and Zhang, L, "Statistical en-route filtering of injected false data in sensor networks", IEEE Journal on Selected Areas in Communications, Volume 23, Issue 4, April 2005, pp. 839 – 850.

[4] Karlof, C., Sastry, N., and Wagner, D., "TinySec: a link layer security architecture for wireless sensor networks", Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 2004, pp. 162 – 175.

[5] Ying, B., Makrakis, D., Mouftah, H. T., & Lu, W. (2011). Dynamic Combinatorial Key Pre-distribution Scheme for Heterogeneous Sensor Networks. In Secure and Trust Computing, Data Management and Applications (pp. 88-95). Springer Berlin Heidelberg.

[6] Kulkarni, S. S., Gouda, M. G., and Arora, A., "Secret instantiation in ad-hoc networks," Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, May 2005, pp. 1–15.

[7] Hamid, M. A., Rashid, M-O., and Hong, C. S., "Routing Security in Sensor Network: Hello Flood Attack and Defense", to appear in IEEE ICNEWS 2006, 2-4 January, Dhaka.

[8] H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, "A game-theoretic approach for high-assurance of data trustworthiness in sensor networks," IEEE 28th International Conference on Data Engineering (ICDE), pp. 1192 –1203, 2012.

[9] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867 – 880, 2012.

[10] Wang, C., Feng, T., Kim, J., Wang, G., & Zhang, W. (2009, June). Catching packet droppers and modifiers in wireless sensor networks. In Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on (pp. 1-9). IEEE.

[11] Ozdemir, S. Secure and reliable data aggregation for wireless sensor networks. In Ubiquitous Computing System; Ichikawa, H., Cho, W.-D., Sato, I., Hee, Y.Y., Eds; Springer:Berlin/Heidelberg, Germany, 2007; pp. 102–109.

[12] Huawei Zhao, Jiankun Hu, Jing Qin, V. Varadharajan and H. Wan, "Hashed Random Key Pre-distribution Scheme for Large Heterogeneous Sensor Networks," Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, Liverpool, 2012, pp. 706-713.

[13] Rasheed, Amar, and Rabi N. Mahapatra. "The three-tier security scheme in wireless sensor networks with mobile sinks." Parallel and Distributed Systems, IEEE Transactions on 23.5 (2012): 958-965.