International Journal of Engineering Research and Technology.
ISSN 0974-3154 Volume 11, Number 2 (2018), pp. 349-371

http://www.irphouse.com

Security Issues in Heterogeneous Network: A review

P.G. Chilveri
Research Scholar, Deparment of Electronics and Telecommunication
Zeal College of Engineering and Research, Savitribai Phule Pune University, Pune, India.
E-mail: pgchilveri@gmail.com
Orcid ID 0000-0001-9316-9849

Dr. M.S. Nagmode
Professor & Head of Department of Electronics and Telecommunication,
Governmentt College of Engineering & Research Avasari,
Savitribai Phule Pune University, Pune, India.
E-mail: manoj.nagmode@gmail.com

Abstract

Wireless sensor networks (WSN) are wireless networks that has some peculiar characteristics because of the lack of infrastructure or executive support. WSN can normally deploy in some of the unattended environments. Recent research topics like IoT model, remote authorized users are allowing in accessing of reliable sensor nodes that has gained data and even more they also allow transferring the commands to nodes that devoted within WSN. However, the sensor nodes are naturally resource constrained, hence it is essential to design a secure, effective and lightweight authentication and key agreement models. Moreover, the heterogeneous network is basically defined as the switching of users from one wireless network to other, and it must also be noticed for its low resources including restricted bandwidth, either low or medium computational ability and energy constraints. Despite these limitations, heterogeneous networking is valuable for situations where communication is desirable. Accordingly, this paper aims to evaluate a review on WSN, heterogeneous networking, and advance communication like Mobile and Adhoc network (MANET). Here, the literature analysis on various model associated with security, privacy preservation, cryptographic models, and key distributions of WSN. It reviews 27 research papers and states the significant analysis. Moreover, this paper provides detailed problem statement of the contributed papers, which extends number of research issues that are useful for the researches to attain further research on security of sensor nodes in WSN

Keywords: WSN; MANET; heterogeneous network; security; privacy preservation

INTRODUCTION

The speedy and widespread enhancement of broadband wireless networks (WNs) has eventually formulated the anticipation of numerous multimedia services, more particularly in mobile environs. However, the prominent network resource managing is a major necessity for aiding many multimedia applications. If the same applications (multimedia) like sports, movies, etc. is requested by multiple users, then a great fall may resist in resources because all users must are in need of a point to point channel [5].This cost-effective need and resources of data (multimedia) delivery have forced the standardization group to provide care for the extensive broadcast and all services of multicast [8] [9].

In general, WSN [35] [36] [43] [45] has been succeeded in many applications like monitoring, military sensing duty and tracking of information, measuring traffic flow, and tracking of environmental pollutant and so on. Naturally, sensor nodes in WSN are devices with resource-constrained that has restricted energy, memory size, and communication ability as well. Since the wireless links are broadcast in nature, the attackers can simply eavesdrop and further can either inject or modify packets, etc. in WSNs. As it is well known that the sensor nodes in WSNs are unavoidable to be cooperated, assuring security in WSNs is even more essential, which is also considered as the urgent task.

The expeditious growth in wireless networks and movable mobile devices in heterogeneous network [29] [30], MANET has expected noteworthy attention. The MANET does not require any fixed setup like the remaining wireless networks in terms of access points of wireless local area networks (WLAN) or base stations of networks. Moreover, in MANET [37], devices (otherwise named nodes) are incorporated to transmit packets on feasible multi-hop paths. The multi-hop path is a network route, which comprises more intermediate nodes among the sending and receiving node. Security [38] [44] in a MANET [31] [32] [33] needs various services like confidentiality, integrity, authentication [39], as well as non-repudiation. The implementation of mobile [40] [41] network also pays better importance in a scheme named Handover (HO) scheme, which is rather important or must be defined in maintaining the continuous communication session while movement of users' from a particular place to another. This is also refers to as the scheme in heterogeneous networking.

HO defines in switching of users' from one Base Station (BS) to another. It performs in the base of definite criteria like service cost, speed of network, QoS, availability that grants by network. Moreover, HO deserves its process in both single and heterogeneous network. For instance, the interworking of networks like 3GPP and WiMAX/WLAN networks is even more striking in terms of performance, because the 3GPP network naturally has its own complementary progression of quality services. Such type of integrated heterogeneous wireless network architecture is defined as Beyond 3G (B3G) or Fourth-Generation (4G) network [11]. Moreover, the heterogeneous HO is basically defined as the switching of users from one wireless network to other, which means a moving person who launches an online chatting

(video) on WiMAX network execute an HO (switching) over other network, 3GPP wireless network. The operations in heterogeneous network perform under definite qualities such as cost, speed and so on, which must guarantee for minimum access cost. However, the user switching from a particular network to another network is not an easy task since it should assure the renowned aspects like best service coverage, secure billing, at minimum cost. Moreover, the network should resist the acquiring attacks that threaten the performance of network, and the most vital aspects which must be considered is authentication [34] [42] of the contributed users. A number of heterogeneous network authentication models is developed to convene the needed security requirements of communication networks. However, the pitfalls like handover latency and delay, computational overhead, etc. are yet to be rectified in the progressing the operation, and still, there is a need for the development of an proficient authentication model for ensuring security.

LITERATURE REVIEW

A. State-of-the-art of contributions

In 2013, KaipingXue *et al*. [1] have specified that WSN could normally deployed in any of the unattended environs. The novel developed IoT model, remote authorized users were allowed for accessing the reliable sensor nodes that have obtained data and even were permitted to transfer the commands to nodes that committed within WSN. Since the sensor nodes were resource constrained in nature, it was necessary for designing a secure, efficient as well as light-weight authentication and key agreement method. This paper has proposed an authentication scheme named Emporal-credential-based mutual authentication approach between the user, GWN as well as sensor node. Moreover, a temporal credential could be issued with the aid of password- centered authentication for every user and sensor node. The outcome of security analysis and performance examination have demonstrated that the developed model could grants moderately high-security features with high security level and at the same time with less overhead in communication, computation as well as storage. Furthermore, it was realistic and well adapted for resource-constrained WSN.

In 2012, E.Ayday and F.Fekri [2] have proposed an authentication scheme to avoid the adversary from overwhelming the infrequent resources of network by inserting bogus packets. The developed authentication scheme progresses on higher reliable as well as energy efficient broadcasting protocol, which was termed as Collaborative Rateless Broadcast (CRBcast). This would enhance the efficiency and reliability of network. The proposed scheme was resilient in terms of Byzantine adversary as well as routing, and also for flooding. The proposed model was compared to other conventional models and has proven the crucial improvement, which has highly ensured the flooding possibility with huge communication overhead and latency.

In 2014, YangYang [3] have proposed an effective encryption scheme called broadcast encryption scheme, which was purely meant for key distribution in MANET. There was no need of message exchanging for group key establishment.

The overhead in communication ruins unmoved even the group size improves. Further, only a single bilinear pairing formulation has required for session key establishment for all group members. The examination has formulated via effectiveness, security study as well as compared with other conventional schemes. The scheme has examined via simulation. The suitability of proposed model for large-scale MANETs was proven from the performance analysis. It has exposed that the developed scheme has proved it's secure in standard model. Moreover, an enhanced model over chosen ciphertext attack (CCA) was developed to improve its security. Hence, it was evident that the developed model could not meet only the security demands, but also it was more efficient in correspondence with both computation as well as communication.

In 2011, ZhijunLi and GuangGong [4] have presented a computationally effective authentication strategy, which was on the basis of learning parity with noise issue. The developed authentication needed only the simplest bit-operations that could make it fit for resource-restrained WSN. The developed model could grant more security relays, which has combined the two 'one-way authentication protocols,' and along with this, it could also grant important improvement in correspondence with possibility of storage or communication necessity. It issues three particular protocols along varied trade-offs among communication overload as well as cost of memory. Further, the performance and security of the developed model were analyzed and proven the superiority of the proposed model.

In 2011, Shengrong Bu *et al*. [5] have studied the dispersed joint authentication as well as intrusion discovery along data fusion in MANETs. They have deployed the Multimodal biometrics to work with a detection system named 'Intrusion Detection Systems (IDSs)' to lighten the defects of uni-modal biometric schemes. More particularly, all devices in the network have some major limitations including measurement and estimation limitations, it was very essential to select some additional devices, and observations could also fused for improving the observation accuracy with the aid of Dempster-Shafer theory for fusion of data. On the basis of security posture, the system adopts whether there was any need for user authentication and which biosensors must be chosen. The decisions were finalized in a complete distributed method by every authentication device and IDS. Further, the simulation outcomes have shown the effectiveness of the proposed model.

In 2013, Fagen Li and Pan Xiong [6] have presented a new heterogeneous online and offline sign cryption scheme. This scheme was developed for securing the communication between a sensor node and the host in Internet. They have proved that the developed scheme was indistinguishable over the adaptive chosen ciphertext attacks over the challenge of 'bilinear Diffie-Hellman inversion problem' and further, existential un-forgability over adaptive chosen messages attacks, especially in random oracle approach. The developed scheme has the upcoming advantages. Initially, it has attained high confidentiality, authentication, and integrity with non-repudiation even in one step. Next to this, it has allowed a sensor node that was based on identity-cryptography for sending a message to the host present on Internet that too in public key infrastructure. Then, the mode has split the sign cryption into two major phases

like offline as well as online phase. In offline phase, dense evaluations were done without the information of a message. Likewise, in online phase, only simple evaluations were done at the availably of message. It was proved that the developed scheme was more suitable for granting security solution mainly for integrating WSN into the IoT.

In 2007, VanesaDaza *et al*. [7] were proposed an Identity-Based cryptography for MANETs, which has provided more security as well. Preceding works have distributed the task of the Private Key Generator (PKG) between the group of nodes in terms of a secret sharing model, whereas the authors have proposed an effective solution for emulating in a dynamic as well as distributed way, and the role of PKG is that even additional nodes connected with the network, it could share the master key of an Identity-Based scheme. This was how the distributed PKG dynamically spreads between the nodes as the improvement made in network. Further, it was proven that the model that has proposed might be fit for further protocols over MANETs.

In 2011, Shengrong Bu *et al*. [8] has stated that the unceasing user authentication was more vital in the prevention-based model for protecting MANETs. Along with this, IDSs were also plays a vital role in MANETs for efficient identify malicious activities. They have formulated the issue as partially observable Markov decision process (POMDP) multi-armed bandit problem for attaining the best model of combining unceasing user authentication and IDSs in a distributed model. They have also presented a structural model for solving the issue of a large network along a diversity of nodes. The policies that were derived from structural outcomes were easy to implement in real time MANETs. The simulation outcomes have shown its efficiency and the performance of developed scheme.

In 2012, Ashok KumarDas *et al*. [9] have reviewed that most of the queries in applications of WSN were issued to the point of either base station or node in gateway of any network. They have proposed a novel scheme named password-oriented user authentication model in hierarchical wireless sensor networks. The developed model has achieved well security as well as efficacy when compared to other conventional password-based models. Along with this, the developed scheme has an advantage of user's password changing dynamically without the aid of base station or gateway node. Moreover, the developed scheme has supported the addition of dynamic nodes in the conventional sensor network.

In 2011, OscarDelgado-Mohatar *et al*. [10] have stated that sensor networks are termed as the ad hoc mobile networks, which were mainly included some sensor nodes along limited formulation and communication abilities. They have also maintained as the economically feasible observing solution particularly for the varied variety of applications. It was identified that the security threats might be addressed in such kind of networks and therefore the authors have developed a light-weight authentication scheme for WSN, which was composed of a key management along authentication protocol. The model was on the basis of simple symmetric cryptographic primitives with fewer formulation needs, and the developed model has attained better outcomes when compared to existing models. When compared to

conventional protocols like SPINS and BROSK protocols, the developed protocol has minimized the consumption of energy up to 98% and 67%, respectively.

In 2009, Xuan Hung Le *et al*. [11] have stated that for varied mission-critical linked WSN applications like military as well as homeland security, it might need for the user's access restriction that could be enforced in the accessing of control appliances for varied access rights. Public key-oriented access control models were smarter than the symmetric-key oriented models in terms of high scalability, fewer memory needs, and so on. Even though, Wang et al. have recently developed an access control scheme that was on the basis of 'elliptic curve cryptography (ECC),' yet it was facing many security limitations especially in providing mutual authentication. This paper has presented an energy-efficient access control model that was based on ECC to overwhelm the above mentioned problems and especially in granting dominant energy-efficiency. The efficiency of the developed model has proven over the conventional models via the analysis and simulation oriented assessments.

In 2011, K. Han *et al*. [12] have analyzed that the initiation of congregated environment that merged with WSNs and mobile networks could be possible in enabling the experience of abundant applications that was on the basis of multi-sensor attached smartphones or devices. Then the authors have developed the authentication protocol, and key agreement protocol, which could minimize the total evaluation and the cost of communication in further generation converged network. The developed security measures were worked via the mobile network for maximizing the lifetime of sensor networks and for the application of joint abilities of both networks. Moreover, the efficiency of developed model has proven over other methods and the developed model could possible in lessening the sensor networks' usage.

In 2010, Hangyang Dai and Hongbing Xu [13] have offered a matrix-related key pre-distribution model for WSN in the defined way: Initially, LU matrix-based model was employed for decomposing the polynomial pool that was substituted for key pool in establishing the shared keys. Secondly, the shared key was evaluated through the shared polynomial. Thirdly, the common polynomials were formulated with mutual authentication. The computational analysis has indicated that the developed approach could allow 100% connectivity irrespective of count of keys. In order to assess the efficacy of network-wide memory overhead, every row or column of L and U matrices were partitioned into two major parts: 'nonzero-element part' and 'zero-element part.' The outcomes have demonstrated that the developed method has granted the references for improving the effectiveness of LU matrix-oriented algorithms. Moreover, with the introduction of polynomial-based key pre-distribution, the resilience over node capture has effectively improved.

In 2009, Manik Lal Das [14] had stated that WSNs were classically arranged in an unattended environ, where the genuine or legitimate users could login to the network and could even access data based on demanding. Subsequently, user authentication was also considered as the primary concern in such resource-constrained environs. With all this consideration, the author has presented a two-factor user authentication protocol for WSN, and that has provided a robust authentication, better establishment

of session key, and also have achieved efficiency.

In 2013, WalidBechkit *et al*. [15] have tackled the resiliency of symmetric key pre-distribution modalities over node capture. They have proposed a hash-oriented model, which has advances the resiliency of key pre-distribution for WSN. The developed model was compared to other conventional methods, and it was proved that the proposed model had granted birth for improved scheme, which was more resilient over some attacks like node capture attacks. The comparison of proposed model over conventional models was carried out in terms of certain vital criteria includes network resiliency over node capture, protected connectivity coverage, storage needs, the overhead of communication and the difficulty of computations as well. The analytical analysis has reviewed that the developed solution has enhanced resiliency of network without the introduction of any storage or communication overheads. Further, it was proved that their solution had introduced the irrelevant computational overhead.

In 2011, William R.Claycomb and Dongwan Shin [16] have presented an approach for protecting WSN, which was on the basis of security policy, imposed at the level of node. The developed policy was on the basis of novel approach of key establishment that has also combined the group-based distribution scheme and identity-oriented cryptography. The developed solution could enable in authentication of nodes with one other, and has granted them with a structure to form a defence communications among one another, and among different groups as well. With the aid of the developed key establishment protocol as well as security policy, it was highlighted the reduction and prevention of significant attacks on WSN.

In 2014, Muhamed Turkanovic *et al*. [17] have focused on some particular environment (interconnection of IoT and WSN) and have developed a new user authentication as well as key agreement model for heterogeneous ad hoc WSN. The developed model has enabled a remote user for securely convey a session key along general sensor node, especially with the aid of lightweight key agreement protocol. The developed scheme has assured the mutual authentication among user, sensor node, and 'Gateway Node' (GWN) as well, even though the GWN has no contact with user. Further, the developed model has revised to the resource-constrained architecture of WSN, and hence, it has utilized only the modest hash and XOR formulations. Moreover, the developed scheme has tackled the hazards and issues posed by IoT, and have assured more security as well as performance features.

In 2014, Soobok Shin *et al*. [18] has stated that the authentication mechanism for accessing legitimate contributors was more essential in pervasive collaboration environs. Hence the authors have presented an effective authentication mechanism for such environments. It was proved that the developed scheme was more secure and was also proved as an effective model via the investigational outcomes that were attained from real-time assessments in pervasive collaboration environment.

In 2006, Roberto Di Pietro *et al*. [19] have introduced a novel threat model for providing confidentiality communications in WSNs, especially against the smart attacker model. Particularly, the security features of the conventional model were

decreasing drastically, and hence they have described a new pseudo-random key pre-deployment approach ESP, which has combined all the defined properties: (i) it cares an energy-efficient key discovery phase, which requires no communications; (ii) it has supported authentication like node to node authentication; (iii) it was extremely resistant to certain smart attackers. They have granted both asymptotic outcomes, and moreover, the extensive simulations of the models were also proposed.

In 2013, QiShi *et al*. [20] have developed a novel lightweight model for rectification of the problem of secure communication. The model has only employed a symmetric cryptosystems for the designing purpose. It has taken the advantage of hierarchical clustering feature for delivering a new way of forming vertical key shareability before the deployment of sensor, and for enabling horizontal key shareability after the deployment (for reliable shared key formation).The evaluation of scheme has evidence that the model has offered better authenticity as well as resilience to diverse security threats, and also has more resource-efficient and scalable over conventional works.

In 2016, Abhijit *et al*. [21] have proposed a handover decision methodology in the Heterogeneous network (HetNet) circumstances which were integrated by the Wifi-Wimax that highly maintained both the user requirements named Quality of experience as well as Quality of service. The HetNet was actually a major concept of next-generation wireless architecture in which several technologies could coexist. Here, the user must have the possibility to select the desired connectivity as per the current situation. The IEEE 802.11 and IEEE 802.16 were the initial building schemes for the HetNet. The authors have reviewed the conventional literature and had understood the interoperability among the technologies and found the defects in the concept of effective utilization of the techniques. The proposed mechanism has solved the problem, and that was proved by analyzing the results of the simulation.

In 2012, Anmin Fu *et al*. [22] had developed a handover authentication approach for WiMax network, which was a group based scheme. The process was when the initial Mobile Station (MS) of the group has moved to the target Base Station (BS) from the service BS; the service BS transferred all the person's security context to the target BS. Hence, the remaining MS in the group could bypass a protocol named Extensible Authentication Protocol (EAP) and allows the security context transmit phase to do the authentication immediately. Therefore, it has ultimately minimized the latency of the handover. Further, the proposed method has achieved the privacy preservation.

In 2012, Thuy Ngoc Nguyen and Maode Ma [23] developed an enhances EAP based pre-authentication scheme (EEP) which have resisted all the vulnerabilities like long delay in consuming time, which was considered as the renowned pitfall of the IEEE 802.16 handover method. The pitfall might cause disruption if the mobile user moved among the base stations. Moreover, another barrier that has mentioned in the method was Denial of service (DoS) with replay attacks. The proposed methodology has solved all the mentioned problems even with minimum requirements on communication as well as computation resources.

In 2011, Ali A. Al Shidhani and Victor C.M. Leung [24] have presented and analyzed the five protocols which were the reauthentication protocols among WLAN and WiMAX using 3G Partnership Project (3GPP) standards. The developed protocol has shown its outstanding performance using reauthentiaction delay and reauthentication signaling traffic. Meanwhile, it has fulfilled the seamless handover (HO) security requirements include frontward and backward secrecy and the mutual authentication provision.

In 2011, Ji Hoon Lee *et al*. [25] had presented an architecture named Multimedia Multicast/broadcast service (MBS) which was based on Location Management Areas (LMAs) that could increase the zone size of the MBS, which could reduce the average handover delay without any loss of bandwidth. Moreover, they have developed an analytical model for the quantification of the server-disruption time, the probability of the blocking and the usage of bandwidth for various MBS zone sizes and LMAs size. Meanwhile, it has considered the distribution of the users, mobility of user, session popularity of MBS. Using the proposed model, they have also proposed how to have the determination of the MBS zones and LMAs finest sizes. Along with this, they have guaranteed the performance of the model. The simulation and analytical results have demonstrated that the proposed LMA based MBS scheme could achieve better efficiency in multicast delivery and at the same time, it could retain the service disruption time.

In 2013, Mohammed A. Ben-Mubarak *et al*. [26] have proposed a self-adaptive handover which was based on fuzzy logic (FuzSAHO). The proposed protocol has overcome the issues like handover delay and handover ping-pong. The proposed algorithm initially self-adapts the parameters of the handover which was on the basis of multiple criteria such as Mobile Station (MS) and Received Signal Strength Indicator (RSSI) velocity. In accordance with the values of handover parameter, the handover decision would be executed. The algorithm was experimented and the results have shown that the proposed algorithm has reduced the handover ping-pong as well as the handover delay.

In 2013, Kuei-Li Huang *et al*. [27] have presented a faster authentication scheme exclusively for mobile stations that roaming within WiMAX-WLAN connected scenario. Moreover, they have incorporated the key reuse design which has prevented the repeated transactions and thereby they have ensured the security while maintaining numerous sites. Additionally, a handover optimization design has been specified in WiMAX for the extension of supporting WiFi-to-WiMAX handovers. The proposed methodology was compared to the conventional schemes, and the analytical and simulation results have shown that the proposed mechanism have leads the position in correspondence with handover packet loss and delay, meeting the requirements of the delay sensitive applications.

Table I. Features and challenges of various authentication scheme

Author	Method	Features	Challenges
KaipingXue *et al*. [1]	Temporal-credential-based mutual authentication scheme	• Less communication as well as computation cost • Suitable for resource constraint WSN	• Key agreement is very simple • Simple key might get hacked
E.Ayday and F.Fekri [2]	Elliptic Curve Digital Signature Algorithm (ECDSA)	• High-performance rate • More reliable	• Only attains average energy consumption • Computation complexity is more
YangYang [3]	Identity-Based Broadcast Encryption (IBBE) approach	• High efficient • Resist adaptively chosen cipher text attack	• Has only limited length • Signature is append to cipher text
ZhijunLi and GuangGong [4]	HB-hybrid framework	• Suitable for resource restrained sensor network • Resist the reflection attack	• Impossible in all applications • Mutual entity authentication is quite difficult
Shengrong Bu *et al*. [5]	Markov chain model	• Enhances the network security • Gains the concept of cross-layer security	• Computation complexity is more • Considered only fewer node states
Fagen Li and Pan Xiong [6]	HOOS scheme	• Reduces the computational cost • Possible to have a	• Requires additional pairing computations • Needs more

		communication among sensor nodes and host in internet	running time for operations like pairing and point multiplication
VanesaDaza *et al*.[7]	Identity-based scheme	• Grants non interactive pairwise key agreement • Shares the master key	• Could hack the key • Some set of nodes are available that could not share the key
Shengrong Bu *et al*. [8]	Partially Observable Markov Decision Process (POMDP)	• Improves the network lifetime • Reduces the information leakage	• Only limited node states are possible • Impossible in all real-time applications
Ashok KumarDas *et al*. [9]	Password-based User Authentication scheme	• Grants better security, • Altering of user's password is possible without having the communication with base station	• Possible to have certain security attacks • Additional requirements are needed for efficient outcome
OscarDelgado-Mohatar *et al*. [10]	Symmetric cryptography	• Depends only on the count of neighbor nodes and not in overall count of nodes in network • Saves the energy up to 98% and 67%.	• Managing of maximum transmission load is a difficult task • Reduces the performance rate.
Xuan Hung Le *et al*. [11]	Elliptic Curve Cryptography (ECC)	• Overcomes the security limitations	• Obtaining practical results is difficult

		• Consumes only less energy	• Implementation in MICA2 motes is impossible
K. Han *et al*. [12]	Generic bootstrapping	• Less energy cost • Minimizes the communication in sensor network	• Implementing in real time 3G-WSN is difficult • Smart grid test bet implementation is also a complex task
Hangyang Dai and Hongbing Xu [13]	Matrix-based key pre-distribution scheme	• Can optimize the memory overhead • Attains higher network connectivity	• Group-based matrix decomposition is difficult • Distributed WSN operation is also a tedious task
Manik Lal Das [14]	Two-factor user authentication protocol	• Less computational cost • Less energy consumption	• Could not resist Deniel of services (DoS) • Threats may occur by node compromise attack
WalidBechkit *et al*. [15]	Hash-based mechanism	• Improves the resilience • Limits the computation overhead	• Unbalanced workload • Possibility of occurring vulnerabilities
William R.Claycomb and DongwanShin [16]	Identity-based cryptography	• Grants node authentication and inter grouping communication • Resist to Sybil attack, wormhole attack and so	• In certain cases, the security of networks is miss-critical to maintain • Delegation between sensor nodes in the security policy is impossible

		on.	
MuhamedTurkanovic *et al*. [17]	Lightweight mutual authentication scheme	• Enables mutual authentication among all parties • Can easily change the password	• Requires more storage space • Additional setup is needed for better result
Soobok Shin *et al*. [18]	Authentication mechanism in ubiquitous collaboration environment	• Evaluation of authentication is an easy task • Less authentication cost	• Need researches for advantaging the next generation • Impossible for ubiquitous collaboration
Roberto Di Pietro *et al*. [19]	Smart attacker model	• Resist Sybil attack • Minimizes the computations and the communications	• Random key pre-distribution schemes are needed • Since sensors are anonymous, security of nodes must be cared
QiShi *et al*. [20]	Lightweight scheme	• Strong authenticity and resilience over various security threats • Resource-efficient in correspondence with computation, communication and memory usage.	• Extension is needed to applicable in other types of sensor network • A real-time application is not so satisfactory.
Abhijit *et al*. [21]	Load balancing and handover policy	▪ Minimizes the communication cost. ▪ Enhances the	▪ Could not control the handovers. ▪ Exact decision

		quality of service (QoS) as well as users'Quality of experience (QoE) of the user.	making is a tedious task.
Anmin Fu *et al*. [22]	Group-based handover authentication scheme	▪ Minimizes the handover latency. ▪ Offers privacy preservation.	▪ Increases the computation overhead. ▪ Computational complexity is high at the initial phase.
Thuy Ngoc Nguyen and Maode Ma [23]	Enhance EAP based pre-authentication(EEP)model	▪ More efficient and secure. ▪ Reduces the delay of handover.	▪ Have more handover latency. ▪ Increases the signaling cost.
Ali A. Al Shidhani and Victor C.M. Leung [24]	HO re-authentication protocol	▪ Reduces the reauthenticati on delay and signaling traffic. ▪ More secure.	▪ Does not support for multihop wireless communication . ▪ Requires additional mechanisms to encounter the errors that occur in protocol.
Ji Hoon Lee *et al*. [25]	Location Management area (LMA) based multicast-broadcast service	▪ Reduces the handover delay. ▪ Grants efficient multicast services.	▪ Additional storing and modeling schemes are required to achieve the efficiency. ▪ Since the popularity increases dramatically, it requires a

			location update triggering.
Mohammed A. Ben-Mubarak *et al*. [26]	Fuzzy logic based self-adaptive handover (FuzSAHO)	▪ Reduces the number of handovers and delay. ▪ Increases the performance rate.	▪ Since it does not consider the interference parameter, there is a possibility of inaccurate decision making. ▪ A real-time application is difficult.
Kuei-Li Huang *et al*. [27]	Fast authentication mechanism (FAME)	▪ Reduces the handover delay. ▪ Improves the security level.	▪ Needs more enhancements for better performance. ▪ More investigation is needed for effective outputs.

B. Problem Definition

Table 1 summarizes the features and challenges of various authentication approaches of heterogeneous network and Fig 1 illustrate the contributed security models. Temporal-credential-based mutual authentication scheme [1] is more suitable for resource constraint WSN with less communication and computation cost, but since the key agreement is simple, it gets hacked easily. Elliptic Curve Digital Signature Algorithm (ECDSA) [2] is more reliable and has high-performance rate. However, it only achieves average energy consumption and has high computational complexity. Identity-Based Broadcast Encryption (IBBE) approach [3] is more efficient and can resist adaptively chosen ciphertext attack, but it has only limited length, and the signature is appended to ciphertext. HB-hybrid framework [4] is suitable for resource restrained sensor network and can resist the reflection attack. However, it is impossible in all applications and also the mutual entity authentication is quite difficult. Markov chain model [5] improves the security of network, but the computation complexity is more. HOOS scheme [6] reduces the computational cost. However, it requires additional pairing computations and also more running time for operations like pairing and point multiplication needs. Identity-based scheme [7] can share the master key, but it could hack the key. Partially Observable Markov Decision

Process (POMDP) [8] enhances the network lifetime. Nevertheless, only limited node states are possible. In Password-based User Authentication scheme [9], the password changing is possible, but additional requirements are needed. Symmetric cryptography [10] can save the energy up to 98% and 67%. However, the managing of maximum transmission load is a difficult task. Elliptic Curve Cryptography (ECC) [11] restricts the limitation of security, but the attaining of real-time results is difficult. Generic bootstrapping [12] requires only less energy, but the smart grid test bet implementation is a tedious task. Matrix-based key pre-distribution scheme [13] has the capability of optimizing memory overhead. However, the implementation in distributed WSN is more complex. Two-factor user authentication protocol [14] could not resist DoS attack and node compromise attack. Hash-based mechanism [15] improves the resilience and limits the computation overhead. Nevertheless, the workload is unbalanced. Identity-based cryptography [16] resist Sybil attack, wormhole attack and so on, but the delegation among sensor nodes in the security policy is impossible. Lightweight mutual authentication scheme [17] needs more storage space. An authentication mechanism in ubiquitous collaboration environment [18] needs only minimum authentication cost, however, it is impossible for ubiquitous collaboration. In Smart attacker model [19], since sensors are anonymous, security of nodes must be cared. Further, in Lightweight scheme [20] extension is necessary to implement in other types of sensor network. Load balancing and handover policy [21] have abundantly increased the quality of service (QoS) as well as Quality of experience (QoE) of the user, and at the same time, it minimizes the cost of communication. Group-based handover authentication scheme [22] ensures the reduction of handover latency, but at the initial phase, computation complexity is very high. Moreover, a model named Enhance EAP based pre-authentication (EEP) model [23] is more secure and efficient. However, the signaling cost is more when compared to other schemes. Even though HO re-authentication protocol [24] requires additional mechanism to solve the errors which occur in protocol, it is more secure. Location Management area (LMA) based multicast-broadcast service [25] reduces the hand over delay and at the same time it grants efficient multicast services, but the thing is it requires a location update triggering. Additionally, Fuzzy logic based self-adaptive handover (FuzSAHO) [26] drastically increases the performance rate but the real-time application of the same is difficult. Fast authentication mechanism (FAME) [27] is a new method which effectively reduces the hand over delay. However, it requires more enhancements for better performance.

RESEARCH GAPS AND CHALLENGES

Even though the heterogeneous network possibly helpful in many aspects; there are some barriers belong to the network in terms of security, and that must be noticed to get effective eco-friendly behavior of network. Usually, the heterogeneous network is a different network that presents various constraints when compared to other conventional computer network. Moreover, sensor networks naturally struggle with specific issues, conventional security techniques utilized in conventional networks could not be smeared directly. Initially, to pose sensor networks economically

feasible, the sensor devices are restricted in their energy, formulation, and communication abilities. Then, unlike other conventional networks, nodes that present in heterogeneous network often deployed with available areas, which must need to overcome the additional risk of physical attacks too. Thirdly, heterogeneous networks cooperate closely with physical environs and with people as well, which poses new security issues, and it must be rectified as soon as possible. Since it has such constraints, it is important to develop some outstanding security mechanisms that satisfy all such constraints.

Additionally, one of the aspects that to be consoled even more effectively is attacks as well as attackers in heterogeneous network. Especially, the outside attacks might make a way of passive eavesdropping while transmitting the data and it could prolong to introducing bogus data into heterogeneous network to consume resources and also has the possibility of raising Denial of Service attacks. Subsequently, inside attackers could harm the network stealthily since they could avoid most of the authentication as well as authorization technique because it acts as the genuine nodes of respective network and has the rights to access the information in network, and the identification of attack patterns are mostly impossible. Further, these attackers could launch different types of attacks including modification, misrouting, snooping or packet dropping. The packet dropping could not be distinguished whether it is dropped by attackers or by genuine nodes. This attack overwhelms the vital information reaching the base station which expressively destroys the performance of networks including rate of packet delivery. Along with this some of the packet dropping attacks very badly struggle in the heterogeneous network, and some of them are Blackhole attack, Grayhole attack, and on-off attacks. These are the severe threat for various applications including military surveillance system that monitors the battlefield and other critical infrastructures. Hence, it is more important to urgently develop some effective approach to enhance the heterogeneous network that free of security issues.

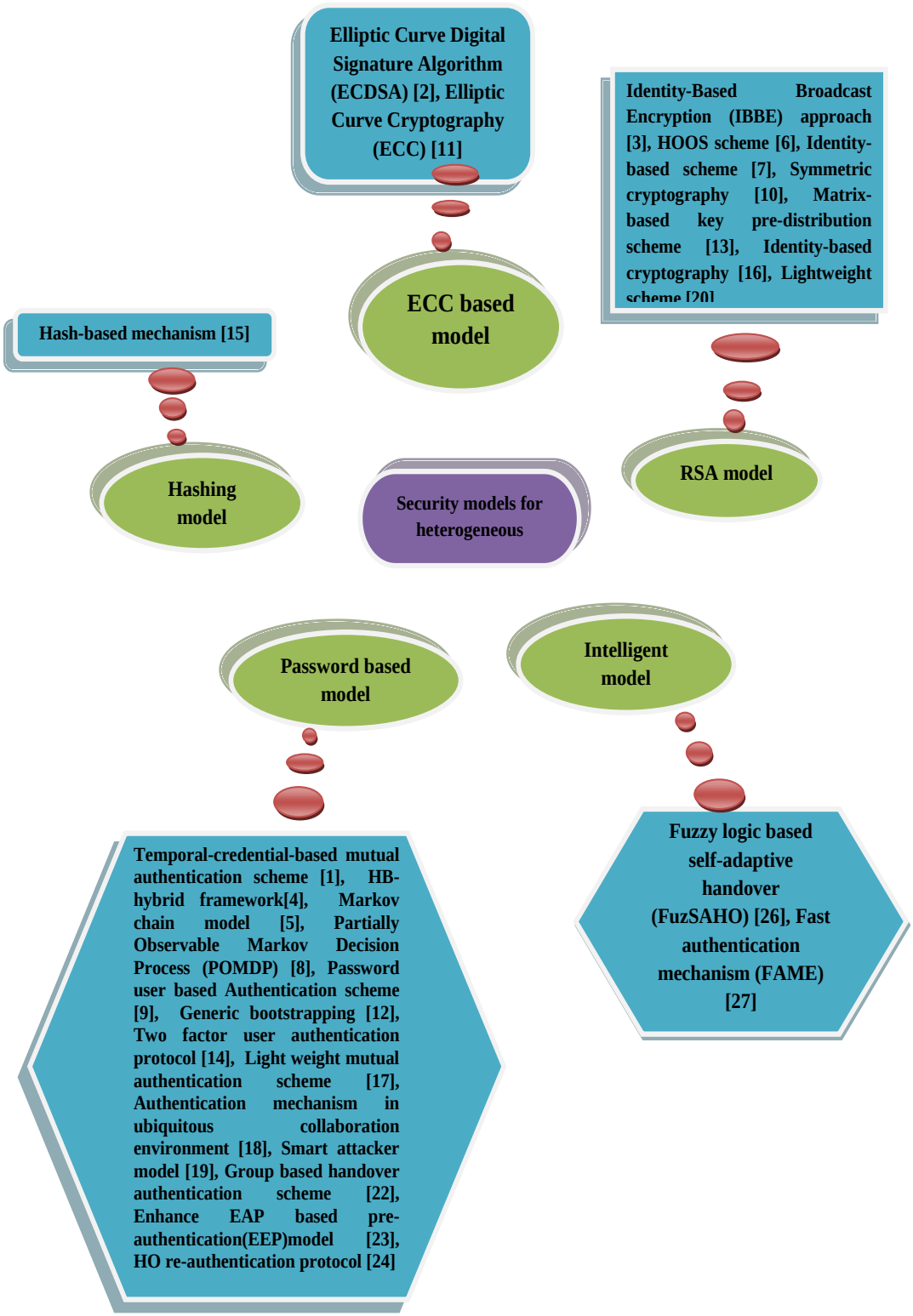

Figure 1. Contributed Security Models

CONCLUSION

From the analysis, it was clear that security of any network is a major concern for providing better performance with less computation and cost as well. This paper has mainly concentrated on security needs in heterogeneous network. Moreover, the MANET networks related with WSN network was mainly analyzed. In this paper, the literature analysed on various characteristics like privacy preservation, confidentiality, authentication services, Hand over latency and delay.

- Consequently, this paper reviewed about 27 research papers and declared the significant analysis
- The review has depicted the overall contribution on different types of security models in heterogeneous network.
- Subsequently, the analysis has reviewed the problem statement of all the contributed security models
- Moreover, the categorization of the respective models was also reviewed detail.

REFERENCES

[1] KaipingXue, ChangshaMa, PeilinHong and RongDing, " A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks", Journal of Network and Computer Applications, vol. 36, no. 1, pp. 316-323, 2013.

[2] E.Ayday and F.Fekri, " A secure broadcasting scheme to provide availability, reliability and authentication for wireless sensor networks", Ad Hoc Networks, vol. 10, no. 7, pp. 1278-1290, 2012.

[3] YangYang," Broadcast encryption based non-interactive key distribution in MANETs", Journal of Computer and System Sciences, vol. 80, no. 3, pp. 533-545, 2014.

[4] ZhijunLi and GuangGong, " Computationally efficient mutual entity authentication in wireless sensor networks", Ad Hoc Networks, vol. 9, no. 2, pp. 204-215, 2011.

[5] Shengrong Bu, F. Richard Yu , Xiaoping P. Liu , Peter Mason and Helen Tang, "Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Ad Hoc Networks", IEEE Transactions on Vehicular Technology , vol. 60, no. 3, pp. 1025 – 1036, 2011.

[6] Fagen Li and Pan Xiong," Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things", IEEE SENSORS JOURNAL", vol. 13, no. 10,pp. 3677-3683, 2013.

[7] VanesaDaza, PazMorillo and CarlaRàfols, " On Dynamic Distribution of Private Keys over MANETs", Electronic Notes in Theoretical Computer Science, vol. 171, no. 1, pp. 33-41, 2007.

[8] Shengrong Bu, F. R. Yu , X. P. Liu and H. Tang, " Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks",IEEE Transactions on Wireless Communications , vol. 10, no. 9, pp. 3064-3072, 2011.

[9] Ashok KumarDas, PranaySharma, SantanuChatterjee and Jamuna KantaSing, " A dynamic password-based user authentication scheme for hierarchical wireless sensor networks", Journal of Network and Computer Applications, vol. 35, no.5, pp. 1646-1656, 2012.

[10] OscarDelgado-Mohatar, AmparoFúster-Sabater and José M.Sierra, " A light-weight authentication scheme for wireless sensor networks", Ad Hoc Networks, vol. 9, no. 5, pp. 727-735, 2011.

[11] Xuan Hung Le , Sungyoung Lee , Ismail Butun , Murad Khalid, Ravi Sankar, Miso Kim, Manhyung Han and Young-Koo Lee, " An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography", Journal of Communications and Networks , vol. 11, no. 6, pp. 599-606, 2009.

[12] K. Han, K. Kim, J. Park and T. Shon, " Efficient sensor node authentication in third generation-wireless sensor networks integrated networks", IET Communications , vol. 5, no. 12, pp. 1744-1754 2011.

[13] Hangyang Dai and Hongbing Xu, " Key Predistribution Approach in Wireless Sensor Networks Using LU Matrix", IEEE Sensors Journal, vol 10, no. 8, pp. 1399-1409, 2010.

[14] Manik Lal Das, " Two-factor user authentication in wireless sensor networks", IEEE Transactions on Wireless Communications, vol. 8, no 3, pp. 1086 – 1090, 2009.

[15] WalidBechkit, YacineChallal and AbdelmadjidBouabdallah, " A new class of Hash-Chain based key pre-distribution schemes for WSN", Computer Communications, vol. 36, no. 3, pp. 243-255, 2013

[16] William R.Claycomb and DongwanShin, " A novel node level security policy framework for wireless sensor networks", Journal of Network and Computer Applications, vol. 34, no. 1, pp. 418-428, 2011.

[17] MuhamedTurkanovic, BoštjanBrumen and MarkoHölbl, " A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion", Ad Hoc Networks, vol. 20, pp. 96-112, 2014.

[18] Soobok Shin, Taeshik Shon, Hongjin Yeh and Kangseok Kim, " An effective authentication mechanism for ubiquitous collaboration in heterogeneous computing environment", Peer-to-Peer Networking and Applications, vol. 7, no. 4, pp. 612–619, 2014.

[19] Roberto Di Pietro, Email authorLuigi V. Mancini, and Alessandro Mei, "

Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks", Wireless Networks, vol. 12, no. 6, pp. 709–721, 2006

[20] QiShi, NingZhang, MadjidMerabti and KashifKifayat, " Resource-efficient authentic key establishment in heterogeneous wireless sensor networks", Journal of Parallel and Distributed Computing, vol. 73, no. 2, pp. 235-249, 2013

[21] A. Sarma, S. Chakraborty and S. Nandi, "Deciding Handover Points Based on Context-Aware Load Balancing in a WiFi-WiMAX Heterogeneous Network Environment," IEEE Transactions on Vehicular Technology, vol. 65, no. 1, pp. 348-357, Jan. 2016.

[22] A. Fu, S. Lan, B. Huang, Z. Zhu and Y. Zhang, "A Novel Group-Based Handover Authentication Scheme with Privacy Preservation for Mobile WiMAX Networks," in IEEE Communications Letters, vol. 16, no. 11, pp. 1744-1747, November 2012.

[23] T. N. Nguyen and M. Ma, "Enhanced EAP-Based Pre-Authentication for Fast and Secure Inter-ASN Handovers in Mobile WiMAX Networks," in IEEE Transactions on Wireless Communications, vol. 11, no. 6, pp. 2173-2181, June 2012.

[24] A. A. Al Shidhani and V. C. M. Leung, "Fast and Secure Reauthentications for 3GPP Subscribers during WiMAX-WLAN Handovers," in IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 699-713, Sept.-Oct. 2011.

[25] J. H. Lee, S. Pack, T. Kwon and Y. Choi, "Reducing Handover Delay by Location Management in Mobile WiMAX Multicast and Broadcast Services," in IEEE Transactions on Vehicular Technology, vol. 60, no. 2, pp. 605-617, Feb. 2011.

[26] Mohammed A. Ben-Mubarak, Borhanuddin Mohd. Ali, Nor Kamariah Noordin, Alyani Ismail and Chee Kyun Ng, "Fuzzy Logic Based Self-Adaptive Handover Algorithm for Mobile WiMAX," Wireless Personal Communications, vol. 71, no. 2, pp. 1421–1442, July 2013.

[27] Kuei-Li Huang, Kuang-Hui Chi, Jui-Tang Wang and Chien-Chao Tseng, "A Fast Authentication Scheme for WiMAX–WLAN Vertical Handover," Wireless Personal Communications, vol. 71, no. 1, pp. 555–575, July 2013.

[28] Kai Zeng, Kannan Govindan and Prasant Mohapatra, " Non-cryptographic authentication and identification in wireless networks [Security and Privacy in Emerging Wireless Networks]", IEEE Wireless Communications, vol. 17, no. 5, pp. 1536-1284, 2010.

[29] Fazirulhisyam Hashim, Kumudu S. Munasinghe and Abbas Jamalipour, " Biologically Inspired Anomaly Detection and Security Control Frameworks for Complex Heterogeneous Networks", IEEE Transactions on Network and

Service Management, vol. 7, no. 4, pp. 268 - 281, 2010.

[30] Yuh-Min Tseng, " A heterogeneous-network aided public-key management scheme for mobile ad hoc networks", International Journal of Network Management, vol. 17, pp. 3-15, 2007

[31] D. Cavalcanti , D. Agrawal , C. Cordeiro, Bin Xie and A. Kumar, " Issues in integrating cellular networks WLANs, and MANETs: a futuristic heterogeneous wireless network", IEEE Wireless Communications, vol. 12, no. 3, pp. 30 – 41, 2005.

[32] Akash Singh, Manish Maheshwari, Nikhil, and Neeraj Kumar, " Security and Trust Management in MANET", Information Technology and Mobile Communication, vol. 147, pp. 384–387, 2011.

[33] Gundala Swathi, Ponugupati Sujala and DR.R.saravanan, " Reducing Communication Overhead For Authentication Using Self Contained Public Key Management Scheme In MANET", International Journal of Engineering and Technology (IJET), vol. 5, no. 3, pp. 2059-2067, 2013.

[34] R. Murugan and A. Shanmugam, " Trust Count Based Authentication Technique for Mitigation of Internal Attacks in MANET", International Journal of Machine Learning and Computing, vol. 2, no. 5, pp. 564-568, 2012.

[35] Huei-Wen Ferng and Nguyen Minh Khoa, " On security of wireless sensor networks: a data authentication protocol using digital signature", Wireless Networks", vol. 23, no. 4, pp. 1113–1131, 2017.

[36] Thomas Newe, Victor Cionca and David Boyle, " Security for Wireless Sensor Networks – Configuration Aid", Advances in Wireless Sensors and Sensor Networks, pp. 1-24, 2010.

[37] Srdjan Capkun, Levente Buttya´ n and Jean-Pierre Hubaux, " Self-Organized Public-Key Management for Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, vol. 2, no. 1, pp. 52-64, 2003.

[38] Hongmei Deng and Dharma P. Agrawal, " TIDS: threshold and identity-based security scheme for wireless ad hoc networks", Ad Hoc Networks, vol. 2, pp. 291–307, 2004

[39] Yuh-Min Tseng, Chou-Chen Yang and Jiann-Haur SU, " Authentication and Billing Protocols for the Integration of WLAN and 3G Networks", Wireless Personal Communications, vol. 29, pp. 351–366, 2004

[40] Raimundo J. Araújo Macêdo and Flávio M. Assis Silva, " The mobile groups approach for the coordination of mobile agents", J. Parallel Distrib. Computing, vol. 65, pp. 275 – 288, 2005.

[41] Levente Buttyan and Jean-Pierre Hubaux, " Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks", Mobile Networks and Applications, vol. 8, pp. 579–592, 2003

[42] Erman Ayday, Farshid Delgosha and Faramarz Fekri, " Data Authenticity and Availability in Multihop Wireless Sensor Networks", vol. 8, no. 2, 2012.

[43] Xuefei Cao, Weidong Kou, Lanjun Dang and Bin Zhao," IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks", Computer Communications, vol. 31, pp. 659–667, 2008

[44] Haowen Chan and A. Perrig, " Security and privacy in sensor networks", Computer, vol. 36, no. 10, pp. 103-105, 2003.

[45] Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, Jonathan Katz and Aram Khalili, " A pairwise key predistribution scheme for wireless sensor networks", Journal ACM Transactions on Information and System Security (TISSEC), vol. 8, no. 2, pp. 44-51, 2005.