International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 17 Issue 2 – SEPTEMBER 2015.

A SECURE TRUST BASED MULTIHOP COMMUNICATION ON WIRELESS NETWORKS

B.Tamil selvi[#1], N.Suresh[*2]

[#1]*M.Phil – Computer Science, Mahendra arts and science college.*

[*2]*M.sc, M.Phil, Department of computer Science, Mahendra arts and science college.*

***Abstract*--Heterogeneous wireless sensor network consists of sensor nodes with different ability.In this project developing a secured environment for detecting malicious nodes in a heterogeneous wireless sensor network.Different abilities such as different computing power and sensing range.With a probability model to analyze the best redundancy level which using path redundancy and source redundancy.The concept of this redundancy management is to exploit the tradeoff between energy consumption with in the gain reliability, timeless and security to maximize the system useful lifetime.In order to improve the method here using heterogeneous node for multipath routing.It uses packet droppers with IDS (Intrusion detection system) for tolerance purpose.To identify packet modifiers,a recently proposed a probabilistic nested marking with certain probability is using.**

IndexTerms:Multipathrouting,Heterogeneous wireless sensor network, intrusion detection, reliability, security, energyconservation

I. INTRODUCTION

The main objective of this project is to develop a secured environment for detecting malicious nodes in a heterogeneous wireless sensor network(HWSN). Here a probability model is used to analyze the best redundancy level, using path redundancy and source redundancy. In order to improve the method here using heterogeneous node for multipath routing.It using packet droppers with IDS(Intrusion detection system) for tolerance purpose.Packet droppers are common attacks that can be launched by an adversary to disrupt communication in wireless sensor networks.Many schemes have been proposed to mitigate the attacks but none can effectively and efficiently identify the intruders.To address the problem,a simple yet effective scheme is proposed,which can identify misbehaving forwarders that drop or modify packets. In a wireless sensor network,sensor nodes monitor the environment,detect events of interest,produce data and collaborate in forwarding the data towards a sink,which could be a gateway,base station,storage node or querying user.

A sensor network is often deployed in an unattended and hostile environment to perform themonitoring and data collection tasks.When it is deployed in such an environment,it lacks physical protection and is subject to node compromise.After compromising one or multiple sensor nodes,an sdversary may launch various attacks to disrupt the in network communication.Among these attacks,two common ones are dropping packets and modifying packets,i.e.,compromised nodes drop or modify the packets that they are supposed to forward.The key conceot is that this redundancy management is to exploit the tradeoff between the energy consumption with the gain in reliability,timeless and security to maximize the system useful lifetime.Formulating the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime.Here it is considering the optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applying to detect and evict malicious nodes in heterogeneous wireless sensor network.

To deal with packet droppers,a widely adopted counter measure is multipath forwarding,in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated.This scheme introduces high extra communication overhead.Another category of counter measures is to monitor the behaviour of forwarding nodes.These schemes are subject to high energy cost incurred by the promiscuous operating mode of wireless interface.To dael with packet modifiers,most of existing counter measures are to filter modified messages within a certain number of hops.Without identifying packet droppers and modifiers,these counter measures cannot fully solve the packet modification problems because the compromised nodes can continue attacking the network without being caught. To identify packet modifiers, Yeet all recently proposed a probabilistic nested marking(PNM) scheme to identify packet

modifiers with a certain probability. However,the PNM scheme cannot be used together with the false packet filtering schemes,because the filtering schemes will drop the modified packets which should be used by the PNM scheme as evidences to inter packet modifiers.This degrades the efficiency of deploying the PNM scheme

Secure data transmission is a critical issue for wireless sensor networks(WSNs).Clustering is an effective and practical way to enhance the system performance of WSNs.Here it is a study of a secure data transmission for cluster-based WSNs(CWSNs),where the clusters are formed dynamically and periodically.We propose two Secure and Efficient data Transmission(SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature(IBS) scheme and the Identity-BasedOnline/Offlinedigital signature (IBOOS) scheme, respectively.In SET-IBS,security relies on the hardness of the Hellman problem in the pairing domain. SET-IBOOS further reduces the com putational overhead for protocol security,which is crucial for WSNs,while its security relies on the hardness of the discrete logarithm problem.We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks.The calculations and simulations are provided to illustrate the efficiency of the proposed protocols.The results show that ,the proposed protocols have better performance than the existing secure protocols for CWSNs,in terms of secutity overhead and energy consumption.It has been proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data,by applying digital signatures to message packets,which are efficient in communication and applying the key management for security.The proposed protocols paring parameters are distributed and preloaded in all sensor nodes by the BS initially

II. MULTIPATH ROUTING

Wireless sensor networks are usually deployed for gathering data from unattended or hostile environment.Several application specific sensor network data gathering protocols have been proposed in research literatures.However,most of the proposed algorithms have given little attention to the related security issues.in this paper we have explored general security threats in wireless sensor network and made an extensive study to categorize available data gathering protocols and analyze possible security threats on them.Due to limitataions of sensor devices,the networks exposed to various kinds of attacks and conventional defences against these attacks are not suitable due to the resource constrained nature of these kinds of networks.Therefore,security inWSNs is a challenging task due to inheritance limitations of sensors and it becomes a good topic for researchers.In this paper we focus at secure routing protocols in wireless sensor networks and surveyed nineteen papers which focusing on this matter.We represent problems and methodologies which are used in order to address the problems.

Advantages in communication technology allow us to build the networks where large numbers of low power and inexpensive sensor devices are integrated in te physical environment and operating together over a wireless media.There are a lot of its application in industry,military and health.In some applications such as intruder detection systems in military,detection of unusual behaviour or failures in a manufacturing process or detection of forest fires,the infrequency of occurrence of specific events has been detected via wireless sensor network(WSN).In the some other WSN applications such as monitoring temperature,humidity and lighting in office buildings,data gathered and reported in the specific periods of time.In some applications scenarios the process of gathering and reporting environment data had been asked through the base,or sink.Insome cases border surveillance,WSN may be used in order to track of specific objects in the environment.

III. SET PROTOCOL

The set protocol module,Secure and efficient data Transmission(SET) protocol for CWSNs.The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency.The proposed SET-IBOOS operates similarly to the previous SETIBS,which has a protocol initialization prior to the network deployment and operates in rounds during communication.We first introduce the protocol initialization,then describe the key management of the protocol by using the IBOOS scheme,and the protocol operations afterwards.

IV. KEY MANAGEMENT FOR SECURITY

This module,the key cryptographies used in the protocol to achieve secure data transmission,which consist of symmetric and asymmetric key based security.

V. NEIGHBOURHOOD AUTHENTICATION

This module is used for secure acess and data transmission to nearby sensor nodes,by authenticating with each other.Here, “limited” means the probability of neighbourhood authentication,where only the nodes with the shared pair wise key can authenticate each other

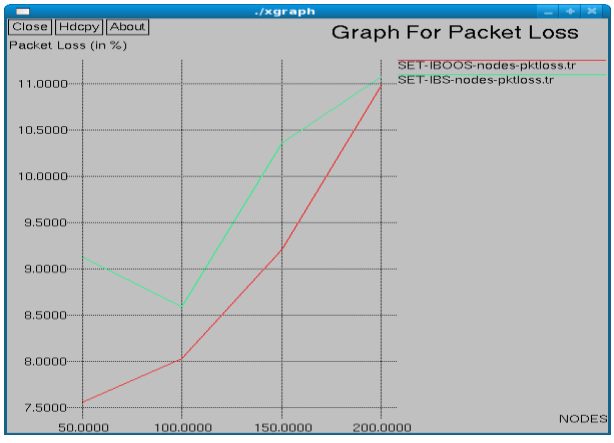
VI. BACKGROUND AND MOTIVATION

Cluster based data transmission in WSNs,has been investigated by researches in order to achieve the network scalability and management,which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes.In acluster based WSN(CWSN),every cluster has a leader sensor node,regarded as cluster-head(CH).A CH aggregates the data collected by the leaf nodes(non-CH sensor nodes)in its cluster,and sends the aggregation to the base station(BS).The LEACH(Low Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelmanetal.It is a widely known and effective one to reduce and balance the total energy consumption for CWSNs.In order to prevent quick energy consumption of the set of CHs,LEACH randomly rotates CHs among all sensor nodes in the network,in rounds.LEACH achieves improvements in terms of network lifetime.Following the idea of LEACH,a number of protocols have been presented such as APTEEN and PEACH,which use similar concepts of LEACH.In this paper for convenience,we call this sort of cluster based protocols as LEACH like protocols.Researchers have been widely studying CWSNs in the last decade in the literature,however,the implementation of the cluster based architecture in the real world is rather complicated.

Adding security to LEACH like protocols is challenging,because they dynamically,randomly and periodically rear-range the network's clusters and data links.Therefore,providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH like protocols(most existing solutions are provided for distributed WSNs,but not for CWSNs).There are some secure data transmission protocols based on LEACH like protocols,such as SECLEACH,GS-LEACHandRLEACH. Mostof them, however, apply the symmetric key management for security, which suffers from a so called orphan node problem.This problem occurs when a node does not share a pair wise key with others in its preloaded key ring,in order to mitigate the storage cost of symmetric keys,and the key ring is not sufficient for the node to share pair wise symmetris keys with all of the nodes in a network.In such a case,it cannot participate in any cluster,and therefore,has to elect itself as a CH.Futhermore,the orphan node problem reduces the possibility of a node joining a CH,when the number of alive nodes owning pair wise keys decreases after a long term operation of the network.Since the more CHs elected by themselves,the more overall energy consumed of the network,the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs.Even in the case that a sensor node does share a pair wise key with a distant CH but not a nearby CH,it requires comparatively high energy to transmit data to the distant CH.The feasibility of the asymmetric key management has been shown in WSNs recently,which compensates the shortage from applying the symmetric key management for security Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems,where the binding between the public key and the identification of the signer is obtained via a digital certificate.The Identity-Based digital signature(IBS) scheme,based on the difficulty of factoring integers from Identity Based Cryptography(IBC),is to derive an entity's public key from its identity information,e.g.,from its name or ID number.Recently,the concept of IBS has been developed as a key management in WSNs for security.Carman first combined the benefits of IBS and key predistribution set into WSNs,and some papers appeared in recent years.The IBOOS scheme has been proposed in order to reduce the computation and storage costs of signature processing,A general method for constructing online/offline signature schemes was introduced by even at all.The IBOOS scheme could be effective for the key management in WSNs.specifically, the offline phase is to be executed during communication.Some IBOOS schemes are designed for WSNs afterwards.The offline signature in these schemes,however,is precompiled by a third party and lacks reusability,thus they are not suitable for CWSNs.

VII. VIBS AND IBOOS FOR CWSN

In this section ,we introduce the IBS scheme and IBOOS scheme used in the paper.Note that the conventional schemes are not specifically designed for CWSNs by distributing functions to different kinds of sensor nodes,based on at first.In order to further reduce the computational overhead in the signing and verification process of the IBS scheme,we adapt the conventional IBOOS scheme for CWSNs,based on.

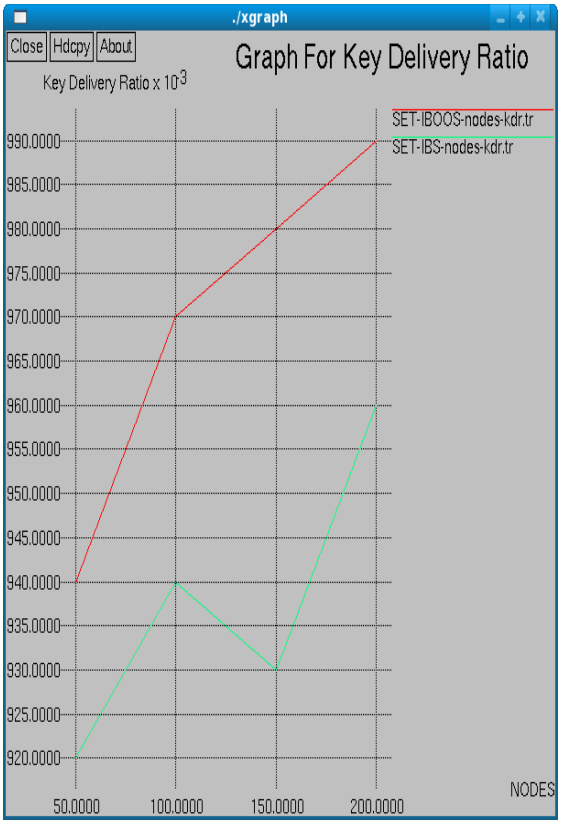


VIII. PAIRING FOR IBS

The first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves.Specifically,randomly select two large primes p and q,and let E/Fp indicate an elliptic curve

y2=x3+ax+b(4a3+27b20)over a finite field Fp.We denote by G1 a q order subgroup of the additive group of points in E/Fp,and G 2aq-order subgroup of the multiplicative group in the finite field F*p.The pairing is a mapping e:G1xG1→G2,which is a bilinear map with the following properties.

1)Bilinear: ∀P,Q,R,S ∈ G1,E(P+Q,R+S) = e(P,R)e(P,S) e(Q,R)e(Q,S).
In the same way, ∀c,d∈Z*q,e(cP,dQ) = e(P,dQ)c = e(cP,Q)d=e(P,Q)cd,etc
2)Non degeneracy:If P is a generator of G1,then e(P,P) is a generator of G2.
3)Computability:There is an efficient algorithm to compute(P,Q)in G2, ∀P,Q ∈G1.
The security in the IBS scheme is based on the bilinear Diffie Hellman Problem(DHP)in th pairing domain,and the hardness of DHP is defined.A bilinear map e is secure if,given g,GH∈G1,it is hard to find h∈G1 such that e(h,H)=e(g,G).Weil pairing and Tate pairing are the examples of such bilinear mapping,which present comprehensive descriptions of how pairing parameters can be selected for security.



IX. PROTOCOL OPERATION

After the protocol initialization,SET-IBS operates in rounds during communication.Each round consists of a setup phase and a steady state phase.We suppose that,all sensor nodes know the starting and ending time of each round,because of the time synchronization.

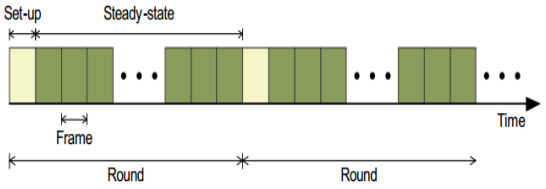


Fig.1.Operation in the proposed secure data transmission

The operation of SET-IBS is divided by rounds as shown in fig,which is similar to other LEACH like protocols.Each round includes a setup phase for constructing clusters from CHs, and a steady state phase for transmitting data from sensor nodes to the BS.In each round,the timeline is divided ichnto consecutive time slots by the TDMA (time division multiple access) control.Sensor nodes transmit the sensed data to the CHs in each frame of the steady state phase.For fair energy consumption,nodes are randomly selected as CHs in each round,and other non CH sensor nodes join clusters using one hop transmission,depending on the highest received signal strength of CHs.In order to elect CHs in a new round,each sensor node determines a random number and compares it with a threshold.If the value is less than the threshold,the sensor node becomes a CH for the current round.In this way, the new CHs are self elected based by the sensor nodes themselves only on their local decisions,therefore,SET-IBS functions without data transmission with each other in the CH rotations.

Setup phase

Step 1. $BS \Rightarrow G_i$: $\langle ID_{BS}, T_s, nonce \rangle$ /* The BS broadcasts its information to all nodes. */

Step 2. $CH_i \Rightarrow G_i$: $\langle ID_i, T_s, adv, \sigma_i, c_i \rangle$ /* The elected CHs broadcast their information. */

Step 3. $L_j \rightarrow CH_i$: $\langle ID_i, ID_j, T_s, join, \sigma_j, c_j \rangle$ /* A leaf node joins a cluster of CH_i. */

Step 4. $CH_i \Rightarrow G_i$: $\langle ID_i, T_s, sched(\ldots, ID_j[t_j, \ldots), \sigma_i, c_i \rangle$ /* A CH i broadcasts the schedule message to its members. */

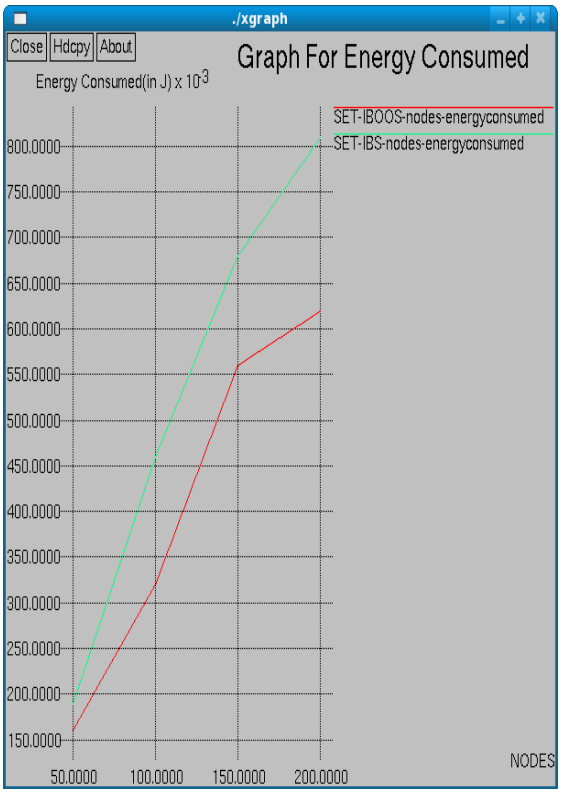
Steady-state phase

Step 5. $L_j \rightarrow CH_i$: $\langle ID_i, ID_j, t_j, C, \sigma_j, c_j \rangle$ /* A leaf node j transmits the sensed data to its CH i. */

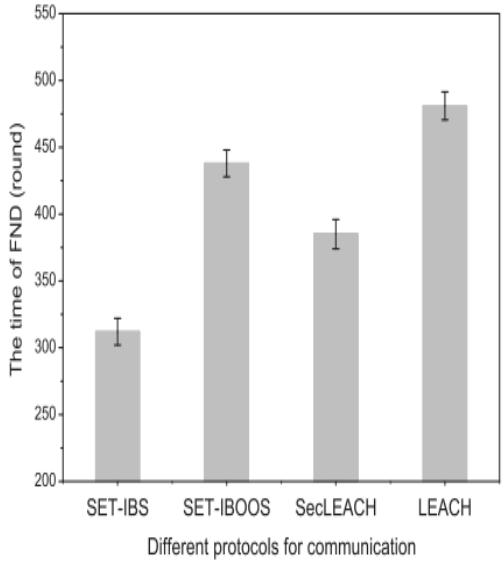
Step 6. $CH_i \rightarrow BS$: $\langle ID_{BS}, ID_i, T_s, F, \sigma_i, c_i \rangle$ /* A CH i transmits the aggregated data to the BS. */

X. SIMULATION RESULTS

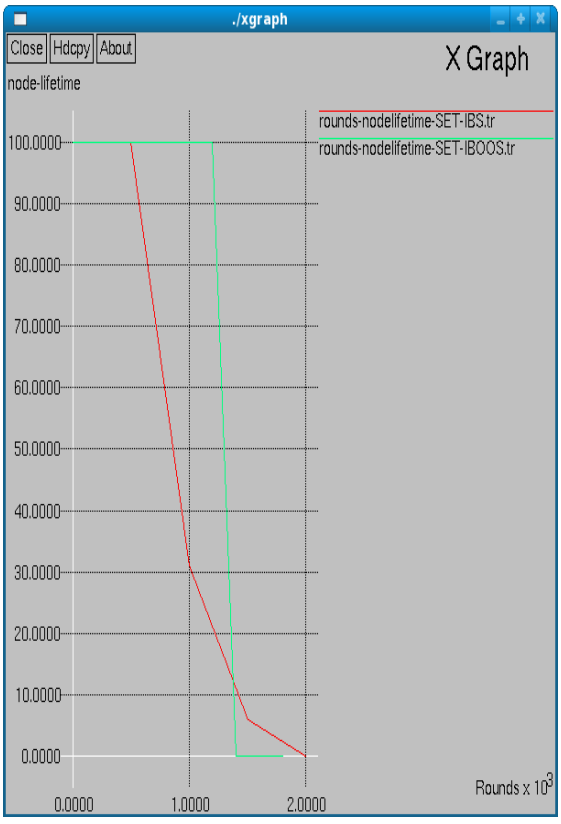
Comprehending the extra consumption by the auxiliary security overhead and prolonging the network lifetime are essential in the proposed SET-IBS and SET-IBOOS.In order to evaluate the energy consumption of the computational overhead for security in communication,we consider three metrics for the performance evaluation:Network lifetime,system energy consumption and the number of alive nodes.for the performance evaluation,we compare the proposed SET-IBS and SET-IBOOS with LEACH protocol and SecLEACH protocol.



Network lifetime(the time of FND)
We use the most general metric in this paper, the time of FND (first node dies), which indicates the duration that the sensor network is fully functional.Therefore, maximizing the time of FND in a WSN means to prolong the network lifetime.

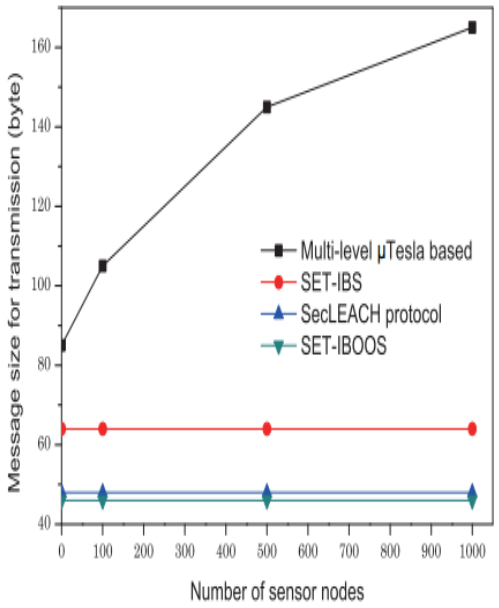


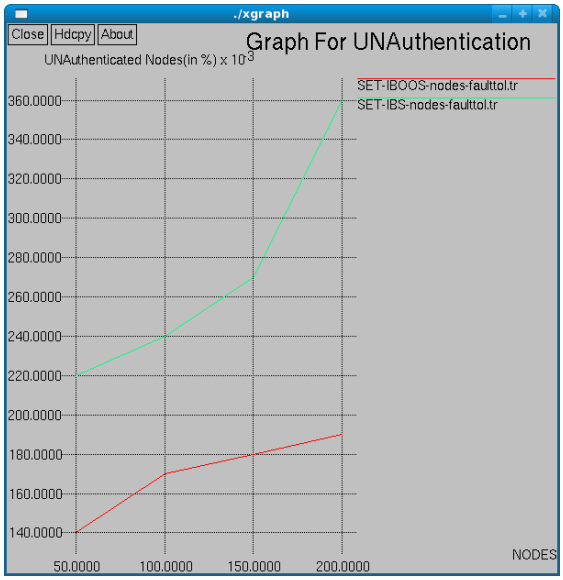
The number of alive nodes
The ability of sensing and collecting information in a WSN depends on the set of alive nodes(nodes that have not failed).Therefore,we evaluate the functionality of the WSN depending on counting the number of alive nodes in the network.



Total system energy consumption

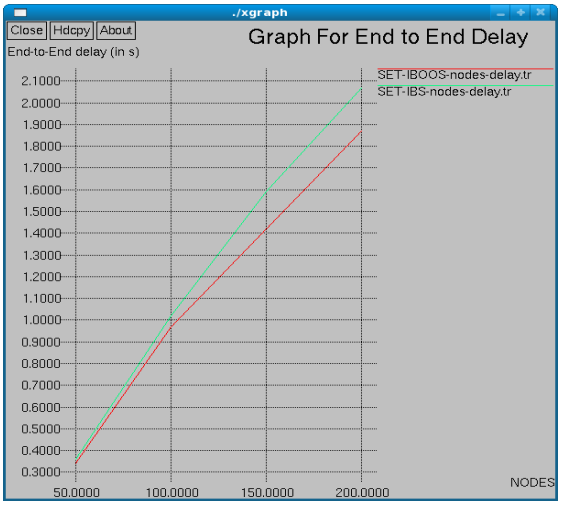
It refers to the amount of energy consumed in a WSN.We evaluate the variation of energy consumption in secure data transmission protocols.In the network simulation experiments,100 nodes are randomly distributed in a 100m X 100m area,with a fixed BS located near part of the area, as shown in the figure





XI. CONCLUSION

In this paper,the data transmission issues and the security issues in CWSNs.The deficiency of the symmetric key management for secure data transmission has been discussed.We then presented two secure and efficient data transmission protocols respectively for CWSNs,SET-IBS and SET-IBOOS.In the evaluation section,we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks.SET-IBS and SET-IBOOS are efficient in communication and applying the ID based crypto-system,which achieves security requirements in CWSNs,as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management.Lastly,the comparision in the calculation and simulation results show that,the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs.With respect to both computation and communication costs,we pointed out the merits that,using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.



REFERENCES

[1]Y.Yang,C.Zhong,Y.Sun,and J.Yang,'Network coding based reliable disjoint and braided multipath routing for sensornetworks',J.Netw.comput.Appl.,vol33,no.4,pp.422-432,2010

[2]R.Machado,N.Ansari,G.Wang,andS.Tekinay, 'Adaptive density control in heterogeneous wireless sensor networks with and without power management, 'IET commun.,vol.4,no.7,pp.758-767,2010

[3]E.Stavrou and A.Pitsillides, 'A survey on secure multipath routing protocols in WSNs, "Comput.New.,vol.54,no.13,pp.2215-2238,2010

[4]T.Shu,M.Krunz,and S.Liu,' Securedata collection in wireless sensor networks using randomized dispersive routes, "IEEE Trans.Mobile Comput.,vol.9,no.7,pp.941-954,2010

[5]Y.Lan,L.Lei, and G.Fuxiang,"A multipath secure routing protocol based on malicious node detection, "in Proc.2009 Chinese control Decision Conf.,pp.4323-4328

[6]Y.Zhou,Y.Fang,andY.Zhang,"Securing wireless sensor networks:asurvey,"IEEECommun.surveys&Tutorials, vol.10,no.3,pp.6-28,2008

[7]D.Somasundaram and R.Marimuthu,"A multipath reliable routing for detection and isolation of malicious nodes in MANET, "in Proc.2008 Int.Conf.Computing ,Commun.Netw.,pp.1-8
[8]H.Su andX.Zhang, "Network lifetime optimization for heterogeneous sensor networks with mixed communication modes," in Proc.2007IEEE Wireless Commun.Netw.conf.,pp.3158-3163
[9] H. Su and X. Zhang, "Network lifetime optimization for heterogeneous sensor networks with mixed communication modes," inProc. 2007 IEEE Wireless Commun. Netw. Conf., pp. 3158–3163.
[10] I. Slama, B. Jouaber, and D. Zeghlache, "Optimal power management scheme for heterogeneous wireless sensor networks: lifetime maximiza-tion under QoS and energy constraints," in Proc. 2007 Int. Conf. Netw. Services, pp. 69–69.
[11] R. Machado, N. Ansari, G. Wang, and S. Tekinay, "Adaptive density control in heterogeneous wireless sensor networks with and without power management,"IET Commun., vol. 4, no. 7, pp. 758–767, 2010.
[12] E. Stavrou and A. Pitsillides, "A survey on secure multipath routing protocols in WSNs,"Comput. Netw., vol. 54, no. 13, pp. 2215–2238, 2010.
[13] T. Shu, M. Krunz, and S. Liu, "Securedata collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, 2010.
[14] Y. X. Jiang and B. H. Zhao, "A secure routing protocol with malicious nodes detecting and diagnosing mechanism for wireless sensor networks," inProc. 2007 IEEE Asia-Pacific Service Comput. Conf.,pp. 49–55.
[15] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," inProc. 2003 IEEE Int. Workshop Sensor Netw. Protocols Appl., pp. 113–127.
[16] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: reliable information forwarding using multiple paths in sensor networks," inProc. 2003 IEEE Conf. Local Computer Netw., pp. 406–415.
[17] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based WSNs
Using ID-Based Digital Signature," inProc. IEEE GLOBECOM, 2010.
[18] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," in
Lect. Notes. Comput. Sc. - CRYPTO, 1990.
[19] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for
AODV and DSR Routing Security," inLect. Notes. Comput. Sc. - Inf. Secur.
Privacy, 2006.
[20] C.-K. Chu, J. K. Liu, J. Zhou et al., "Practical ID-based encryption for wireless
sensor network," inProc. ACM ASIACCS, 2010.
[21] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and
countermeasures,"Ad Hoc Networks, vol. 1, no. 2-3, 2003.
[22] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," inLect.
Notes. Comput. Sc. - SAC, 2003.
[23] J. Liu and J. Zhou, "An Efficient Identity-Based Online/Offline Encryption
Scheme," inLect. Notes. Comput. Sc. - Appl. Crypto. Netw. Secur., 2009.
[24] J. J. Rotman, An Introduction to the Theory of Groups. Springer-Verlag; 4th
edition, 1994.
[25] K. S. McCurley, "The discrete Logarithm Problem," inProc. Symp. Appl. Math.,
Prog. Com. Sc., 1990, vol. 42.
[26] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf.
Theory, vol. 22, no. 6, 1976.
[27] D. Boneh, I. Mironov, and V. Shoup, "A Secure Signature Scheme from Bilinear
Maps," inLect. Notes. Comput. Sc. - CT-RSA, 2003.
[28]P.Barreto,H.Kim,B.Lynn et al.,"Efficient Algorithms for Pairing-Based
Cryptosystems," inLect. Notes. Comput. Sc. - CRYPTO, 2002.
[29]C.Castelluccia,E.Mykletun,and G. Tsudik, "Efficient aggregation of encrypted
data in wireless sensor networks," inProc. MobiQuitous, 2005.
[30]H.Lu, J. Li, and G. Wang, "A Novel Energy Efficient Routing Algorithm for
Hierarchically Clustered Wireless Sensor Networks," inProc. FCST, 2009