ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Multipath Routing Scheme for Wireless Network: A Review

Namrata P. Mishra[1], Samadhan D.Mali[2]

PG student, Digital Systems (Electronics), SCOE, Pune, India[1]

Assistant Professor, Dept. of E&TC, SCOE, Pune, India[2]

ABSTRACT: In any wireless sensor network detection of compromised node is very important. It has affected the reliability and efficiency of wireless sensor network. False report will embed in the system by means of nodes which are compromised. These false reports create false alarms in the battery fuelled framework.The false data implantation in a Cyber physical network system is accomplished by network of cluster. In this paper, we have reviewed and analyzed different methods which detect faults results created by compromised nodes. Therefore it is very important to find out the route which maximize end to end throughput. Therefore Spatial Reusability Routing is discussed.

KEYWORD*:* Spatial Reusability Routing, Multipath, SAAR routing protocol, wireless sensor network, etc.

I. INTRODUCTION

In this paper themethodology which used the polynomials known as Polynomial-based Compromised-Resilient En-route Filtering for Cyber-Physical Networked Systems is introduced. This method filters false data and provides high security to the number of nodes which are under malicious condition, which doesn't relies on the stable data circularize path and node determination. PCREF utilizes polynomials rather than MACs to check reports. In this method, nodes are defined with probability and authentication message is send to these nodes.Therefore this approach can't operate upon stable path. Hence it is very important to find out the route which maximize end to end throughput. Therefore Spatial Reusability Routing is discussed.

There are many types of filtering schemes in wireless sensor network. Every scheme has different feature. A list of different filtering schemes and their abbreviations are given below:

1. PCREF(Polynomial-based Compromised-Resilient En-course Filtering)
2. SEF(Statistical En-routing filtering)
3. IHA(Interleaved Hop-by-Hop Authentication scheme)
4. LBRS(Location based routing scheme)
5. LEDS(Location aware end to end data security)
6. CCEF (Cipher based En-route Filtering scheme

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

II. LITERATURE SURVEY

Xinyu Yang_, Jie Lin, Paul Moulemay,WeiYuy, XinwenFuz and Wei Zhao "A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems".[1] This paper describes that, In cyber physical network system different polynomials are used to detect the false data.

Z. Yu. And Y. Guan,"A dynamic en-route filtering scheme for data reporting in wireless sensor networks"[2].In this paper the detection of false data and Dos attacks in the wireless sensor network are done with the help of hash chain.

S. Zhu, S. Setia, "An interleaved hop-by-hop authentication scheme for filtering of injection false data in sensor networks" [3]. This work proposes adifferent authentication method to prevent false injection attack in wireless sensor network.

F. Wu, Y. Kao, and Y. Tseng, "From wireless sensor networks towards cyber physical system" [4]. This work proposesnetworking issues and coverage and deployment issues.

H. Yang and S. Lu. "Commutative cipher based en-route filtering in wireless sensor networks" [5]. This work describes that fabricated reports are en-route without symmetric key sharing in wireless sensor network. In CCEF, the association is developed between source node and base station while the intermediate forwarding nodes are equipped with a witness key.

F. Ye, H. Luo, S. Lu, and L. Zhang."Statistical en-route filtering of injection false data in sensor networks"10].This work proposes the SEF i.e. Statistical en-route filtering scheme which detect and notproceed with that false reports. SEF check the each report and by multiple keyed messages authentication codes (MAC).

H. Yang, F. Ye, Y. Yuan, S. Lu, and **W. Arbaugh**. "Toward resilient security in wireless sensor networks"[9]. This work proposes that LBRS utilize location based keys to filter false report. It assumes that sensor nodes can determine their location in short time, but practically it is not possible.

K.Ren, W. Lou, and Y. Zhang."LEDS**:** Providing location-aware end-toend data security in wireless sensor networks" [7]. This work proposes that LBRS utilize location based keys to filter false report. It assumes that sensor nodes can determine their location in short time, but practically it is not possible. A key feature of directed diffusion is that every sensor node can be aware, which means that nodes store and interpret interest packets, rather than merely forwarding them along the route.

III. METHODOLOGIES

The different methods are discussed below, which detects fault results created by compromised nodes in the wireless sensor network. Because node compromise intended various security issues in wireless sensor network. Adversaries can also inject false data reports through compromised nodes. There are various methods are available which filters the false data such as statistical En-routing scheme, IHA,CCEF,LBRS,LEDS,RPB.

1) Polynomial based compromised resilient En-routing filtering scheme

The basic idea of Polynomial based compromised resilient En-routing filtering method is described below. PCREF utilizes polynomials instead of MACs. PCREF uses polynomials. These polynomials are divided into two types i.e. i)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Authentication polynomial ii) Check polynomial. These polynomials are obtained from primitive polynomial and stored in nodes with node ID. Each sensing node stores the authentication polynomial of the local cluster and stores the check polynomial of other clusters with a pre-defined probability P. Each forwarding node stores the check polynomial of each cluster with the same probability P. PCREF is divided into two main parts i.e. i) Authentication information management. ii) Data security management.In authentication information management various functions are carried out such as assign the key, authentication polynomial, check polynomial, and local ID of sensing nodes, whiledata security management is used to detect and filter the false measurement reports.Node localization and static data dissemination routes play an important role in PCREF regarding to resilience of compromised nodes. PCREF also uses T-authentication framework which means that legitimate report shall be authenticated by T nodes from the same cluster. Forwarding node could verify the report only if it shares the authentication information with the source nodePCREF adopts polynomial instead of MAC messages to verify reports. PCREF achieve better performance than SEF, LBRS, and GRSEF & LEDS.

2) Statistical En-routing filtering (SEF)

Statistical en-route filtering is independent of network topology. This scheme takes advantage of the large-scale and dense deployment of sensor networks. In Statistical en-route filtering, the detection and filtration of false reports is increases with increase in deployment of sensor networks. In Statistical en-route filtering, the detection of false reports can be done even if the attacker know the security keys provided that these keys obtained from compromised nodes to a small number of the key pool partitions.In Statistical en-route filtering, the maximum false data is filtered from compromised nodes near about in 10 forwarding hops. In this method the false report detected by the decision of the multiple sensor and security information is also assigned to the multiple sensors instead of single node and these multiple sensors generate legitimate report. The legitimate report contains multiple Message Authentication Codes (MACs).Each forwarding node checks the correctness of the Message Authentication Codes (MACs). If incorrect MAC is detected, the report is dropped. The chances of detecting incorrect MACs increases, as the reports travels from number of hops. Depending on the path length, there is a non-zero probability that some reports with incorrect MACs may escape en-route filtering and be delivered to the sink. In Statistical en-route filtering, the sink will further check the correctness of each MAC carried in each report and reject false ones. Collaborative filtering of false reports requires that nodes share certain amount of security information.SEF has limited filtering capacity, and SEF cannot prevent the impersonating attack.

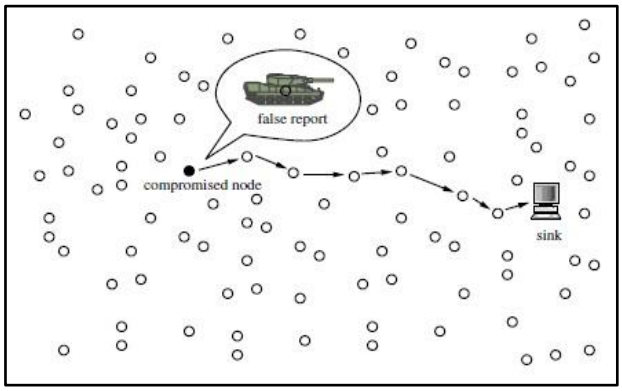

Fig.1Example of a false report sent to sink via compromised node. [10]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

3) Interleaved Hop-by-Hop Authentication scheme

Whenever sensornetworks are introduced in unattended environments. There are greater chances that these networks are vulnerable to falsedata injection attack. In this scheme the interleaved hop-by-hop authenticationmechanism. Base station will detect any injected false data packets only when the numbers of compromised nodes are not greater than t nodes. The base station can detect false data only when number of nodes is not more than t nodes. i.e. Any injected false data packets when no more than a fix en number sensor nodes are vulnerable to attacker. Further, this scheme provides an upper bound B for the number of hops that a false data packet could be forwarded before it is detected and dropped.

4) Random Perturbation-Based scheme

The communication between two sensor nodes is secure only when these nodes share a pair-wise key. In this scheme any two nodes can directly established a pair-wise key without exposing any secret to another nodes. In this scheme if large number nodes have been compromised, the pair-wise key shared by non-compromised nodes are remains secure. This schemes implements polynomial to generate pair-wise keys. The pair-wise polynomials are alsoused in Random Perturbation-Based scheme. These pair-wise polynomials generate pair-wise keys and the polynomials are defined over finite field.

5) Resilient Security in wireless sensor network

Compromise nodes impose the security issues in wireless sensor network. The existing security methods in wireless sensor network, introduced only for small and fix threshold number of compromised nodes. This security is broken when this threshold isexceeded than fixed threshold. In this scheme the limitation of threshold and achieve the resilience y against compromised nodes.In this scheme the location based method is used.Each node stores a few keys based on its own location. This scheme limiting the damages happened due to compromised nodes.

6) Dynamic En-Route Filtering Scheme

In Dynamic En-Route Filtering Scheme the false data and Dos attacks are discussed. In this scheme, hashchain ofauthentication keys are utilized by each node. This key is disseminated by each node towards forwarding node. The sending nodes disclose their key after completion of sending the reports.The cluster-head scatters the authentication-key of every node to forwarding nodes and then sends the reports with disclosed authentication-keys. The forwarding nodes confirm the authenticity of the disclosed keys by hashing the disseminated keys. The forwardingnodes not only confirm the authenticity but also and then check the legitimacy of the reports using the disclosed keys. After the validation of reports, they inform the next-hop nodes to either drop or keep on forwarding the reports. This process is repeated by each forwarding node at every hop.There are various advantages of this scheme. This scheme can drop false reports considerably prior even with a littler size of memoryThe uncompromised nodes will not be impersonated because each node has its own authentication-keys. Therefore, once the compromised nodes are detected, the infected clusters can be easily quarantined. This approach increases filtering capacity greatly and balances the memory requirement among nodes. This scheme is adaptive to highly dynamic networks and also mitigates the impact of selective forwarding attacks. Monitored by its upstream nodes and neighbours, the compromised nodes have no way to contaminate legitimate reports or generate false control messages.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

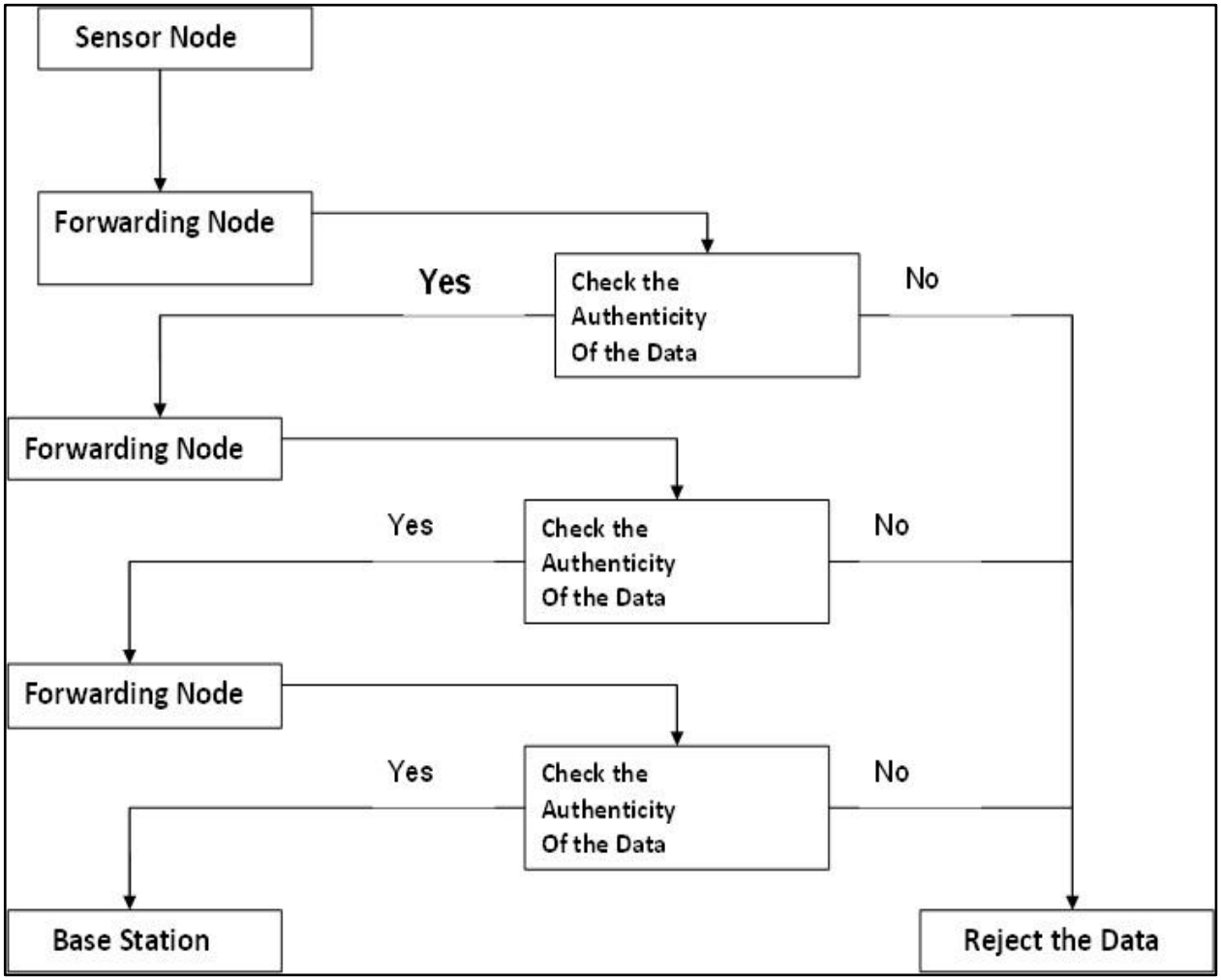

Fig.2Dynamic En-routing filtering scheme [2]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

IV. ADVANTAGES AND DRAWBACKS OF EN-ROUTING FILTERING SCHEMES

Table 1Advantages and Drawbacks

Sr. No	Schemes	Advantages	Drawbacks
1.	PCREF	1) Filtering efficiency of PCREF is highest than SEF, LBRS, and LEDS 2) Filtering capability is better than above stated methods. 3) PCREF achieves high resilience than SEF	1) Static path is required.
2	SEF	1) Filters 80% false data by a compromised node within 10 forwarding hops.	1) Collaborative Filtering of false report is not possible.
3	Dynamic En-Routing scheme.	1) Drop false report earlier 2) Uncompromised nodes are not impersonate 3) Increased filtering capacity	1) More complicated 2) Control messages can be abused. 3) Delay of report

V. CONCLUSION

In this paper we have presented a comprehensive review of few important En-routing filtering schemes such as PCREF, SEF, IHA, RPB and Dynamic En-routing scheme. This paper analyzed these schemes based on routing and filtering. Detection of faulty nodes between wireless sensor networks to avoid attacks, the secure routing protocol should be used such that a network continues to function properly.PCREF provide different polynomials to ensure secure and energy efficient packet transmission. In this system cluster based polynomials are assigned to avoid effect of compromised nodes. To enhance this work proposed system developed trust based secure signature for the wireless sensor as authentication scheme. Trust based signature ensure sensor node for sensor energy and identity in the network. Digital signature is kind to verify wireless sensor security in form of node identity and trust value which is computed with energy level of sensor nodes.The proposed scheme also contributes for shortest path communication between end to end nodes in network. This computation uses SASR and SAAR routing protocol for energy efficient packet transmission. This protocol ensure to reduction of overhead for packet transmission at end to end node in the network.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

REFERENCES

[1] Xinyu Yang,Jie Lin, Paul-Marie Moulema,Wei Yu Xinwen Fu and Wei Zhao "A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems" IEEE Transaction on computers, VOL. 64, No. 1, January 2015.
[2] Z. Yu. And Y. Gaun, "A dynamic en-route filtering scheme for data reporting in wireless sensor networks," IEEE Transactions networking, Vol. 18, pp. 150-163, 2010.
[3] S. Zhu, S. Setia, "An interleaved hop-by-hop authentication scheme for filtering of injection false data in sensor networks," ACM Transaction sensor Network, Vol. 3, no. 4, pp. 259-271, 2007.
[4] F. Wu, Y. Kao, and Y. Tseng, "From wireless sensor networks towards cyber physical system," Pervasive mobile computer., Vol. 7, no. 4, pp. 397-413, Aug. 2011
[5] H. Yang and S. Lu. "Commutative cipher based en-route filtering in wireless sensor networks". In Proc. of 60th IEEE VTC, 2004.
[6] Y.-S. Chen and C.-L. Lei. "Filtering false messages en-route in wireless multi-hop networks". In Proc. of IEEE WCNC, 2010.
[7] K. Ren, W. Lou, and Y. Zhang. "Leds: Providing location-aware end-to-end data security in wireless sensor networks. IEEE TransactionMobile Computing (TMC), 7(5):585–598, 2008.
[8] N. Subramanian, C. Yang, and W. Zhang. "Securing distributed data storage and retrieval in sensor networks". In Proc. of the 27th IEEEInternational Conference on Pervasive Computing and Communications(PerCom), 2007
[9] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh. "Toward resilient security in wireless sensor networks". In Proc. of the 6th ACM Int,Sys Mobile Ad Hoc Netw.compu. (MobiHoc'05), 2005.
[10] F. Ye, H. Luo, S. Lu, and L. Zhang. "Statistical en-route filtering of injection false data in sensor networks". In Proc. of the 23th IEEEINFOCOM, 2004.
[11] L. Yu and J. Li. "Grouping-based resilient statistical en-route filtering for sensor networks". In Proc. of the 28th IEEE INFOCOM, 2009.
[12] W. Zhang, N. Subramanian, and G. Wang. Lightweight and compromise resilient message authentication in sensor networks. In Proc. of the 27thIEEE INFOCOM, 2008.
[13] W. Zhang, M. Tran, S. Zhu, and G. Cao. "A random perturbation-based pairwise key establishment scheme for sensor networks". In Proc. of the8th ACM MobiHoc, 2007.
[14] S. Zhu, S. Setia, S. Jajodia, and P. Ning. An interleaved hop-by-hop authentication scheme for filtering of injection false data in sensor networks. In Proc. of the 25th IEEE Symposium on Security and Privacy(S&P), 2004.