DOI:10.13203/j.whugis2008.10.028
第33卷 第10期 武汉大学学报·信息科学版 Vol.33 No.10
2008年10月 Geomatics and Information Science of Wuhan University Oct. 2008

文章编号:1671-8860(2008)10-1042-04 文献标志码:A

能量有效的无线传感器网络安全拓扑控制协议

王新胜[1] 詹永照[1] 王良民[1,2]

(1 江苏大学计算机科学与通信工程学院,镇江市学府路301号,212013)
(2 东南大学计算机科学与工程学院,南京市四牌楼2号,210018)

摘 要:节能和安全是无线传感器网络应用中的一对矛盾需求,为调和这对矛盾,提出了一种能量有效的无线传感器网络安全拓扑控制协议(energy-efficient secure topology control protocol, ESTCP)。ESTCP首先根据节点地理位置形成结构化的网格拓扑;其次,通过单向哈希密钥链技术和对称密钥认证技术控制新节点在不同情形下的安全加入,通过新节点间形成临时簇减少因认证新节点带来的能量损耗。分析和仿真表明,ESTCP在较少的资源开销下有效保证了拓扑控制的安全性。

关键词:传感器网络;拓扑控制;安全
中图法分类号:TP393

无线传感器网络(WSN)的拓扑控制安全由于其在特殊应用中特别是军事应用中的重要性,因而引起了广泛关注。目前拓扑控制中新节点加入的安全性详细研究国内外较少,文献[1]简单讨论了节点加入网络的安全,但只涉及了节点的身份认证。文献[2]考虑了新节点如何安全加入,但仍存在敌手伪装成新节点发动DoS[3]攻击问题。能量问题是WSN研究的焦点问题,而拓扑控制是能够减少能量消耗的最重要的技术之一[4]。文献[5-7]提出了基于六边网格拓扑的WSN,该网络通过设计结构化的网络拓扑、利用冗余节点储存能量,有效地延长了网络的生命周期,但它们在拓扑控制方面缺乏安全性设计等问题。

1 预备工作

本文给出安全协议所使用的前提假设:① 假定在部署阶段每个节点能获取自己的地理位置。安全定位是一些特殊应用中最基本需求,文献[8,9]中讨论了相关问题,因此,本安全协议并不因该假设增加额外开支。② 假定在部署阶段,WSN处于完全安全状态,敌方无法俘获我方节点,已有的WSN安全协议[9]同样持有该假设。③ 假定在后继新节点播撒阶段,新节点在短时间内处于安全状态,敌方无法俘获我方新节点,文献[2]持有同样类似的假设。

本文使用了下列符号定义描述文中的安全协议和加密操作:RC表示含冗余节点的正六边形单元;AN表示RC单元内工作的活动节点;K_s表示基站与每个节点的共享对称密钥;K_{is}表示新节点间的临时公共对称密钥;ID_i表示RC中一个节点i,ID_0代表基站,ID_{in}表示RC中以ID_i为簇头的所有节点;$MAC_{ij}(M)$表示使用ID_i与ID_j共享的对称密钥生成信息M的认证码;$MAC_k(M)$表示使用K_{is}生成信息M的认证码;定义:设G为节点的坐标集合,存在$(x,y)\in G$,对任意$(x_0,y_0)\in G$且(x_0,y_0)不同于(x,y),若(x,y)满足$x<x_0$或$x=x_0$且$y<y_0$,则称(x,y)是G的最小坐标,记作$\min_G(x,y)$。

2 安全拓扑控制协议ESTCP

ESTCP包含以下两个方面:① 拓扑的生成,主要实现由初始随机播撒节点如何构建结构化的网络拓扑;② 新节点的加入,主要实现如何将后继新播撒节点加入到已有的结构化网络拓扑中。

收稿日期:2008-08-28。
项目来源:国家自然科学基金资助项目(60703115);国家博士后专项基金资助项目(20070420955);江苏省自然科学基金资助项目(BK2007560);江苏省博士后科研计划资助项目(0702003B);江苏大学高级人才科研启动经费资助项目(07JDG080)。

2.1　拓扑生成

节点被播撒到目的地后,通过广播通信构建逻辑上由六边形单元组成的结构化的网络拓扑,拓扑构建过程分为以下三个阶段。

1) 初始化阶段。首批播撒节点预存 K_s、RC 半径 r 和播撒批次 K_0。播撒后,节点通过 GPS 定位系统获得各自位置并以距离 $2r$ 向周围广播,这样每个节点获得了所有邻居节点的位置。

2) RC 分割。本文采用和文献[6]相类似的方法确定节点所隶属的 RC。基站(BS)广播包含其坐标和 r 的分割信息给周围节点,当节点收到分割信息后,计算出周围 RC 的中心坐标,根据这些值和自身的位置计算出离哪个 RC 中心点最近,离得最近的 RC 就是该节点所隶属的 RC。

3) AN 选择。设 G 为 RC 内所有的节点集合,找出坐标为 $\min_G(x, y)$ 的节点,该节点即为 AN,随后其他节点进入睡眠状态。每到一个睡眠间隔时间 T_s,睡眠节点就发送一个询问信息给 AN,来决定自己继续睡眠还是替换 AN 进行工作。

2.2　新节点的加入

2.2.1　新节点加入有 AN 的 RC

1) 新节点的确认。本文提出一种基于单向哈希密钥链的新节点认证技术,通过比较已有节点的单向哈希密钥和新节点的单向哈希密钥之间的关联性,确认要加入节点是否为新节点。该技术包括以下四个步骤。

① 新节点初始化。在部署前,新节点预存如下信息:本次播撒批次 K_v、K_s、K_{ts}、r 和 BS 坐标。

② 新节点之间的基于 K_{ts} 确认过程:新节点 ID_i 产生报文 $P_i(K_v, ID_i, MAC_k(ID_i))$,并广播给 RC 中其他新节点。其他新节点通过比较 K_v 确定 P_i 是否是同批次播撒的新节点发送。

③ 新节点间临时簇头的选择。设 G 为 RC 内所有新节点集合,找出坐标为 $\min_G(x, y)$ 的新节点,该节点即为临时簇头。

④ 临时簇头与 AN 之间的确认过程。临时簇头 ID_i 产生报文 $P_i(K_v, ID_{in}, MAC_{i0}(ID_{in}))$,如图 1 中①所示,$ID_i$ 将 P_i 广播给播撒批次为 K_j 的 ID_j。若 $K_j = F^{w-j}(K_v)$,其中 F 为单向哈希函数,则 ID_j 确认 ID_{in} 中节点为新节点。

2) 新节点合法性确认。活动节点 ID_j 需要进一步通过 BS 来确定新节点 ID_i 的合法身份,其步骤如下。

① ID_j 生成报文 $P_j(ID_j, ID_{in}, MAC_{i0}(ID_{in}), MAC_{j0}(ID_j, ID_{in}, MAC_{i0}(ID_{in})))$;如图 1 中②所示,$ID_j$ 将 P_j 传递给 BS。

② BS 接收 P_j 并验证 P_j 和 ID_{in},如果合法,BS 生成 $P_0(ID_j, MAC_{j0}(ID_j), MAC_{0j}(ID_j, MAC_{i0}(ID_j)))$,如图 1 中③所示,BS 发送 P_0 给 ID_j。

③ ID_j 接收 P_0 并验证 P_0,如果合法,ID_j 接受 ID_{in} 为本 RC 节点,如图 1 中④所示,ID_j 发送确认报文 $P_t(ID_j, MAC_{i0}(ID_j))$ 给 ID_i。

④ ID_i 接收 P_t 并验证 P_t,如果合法,接受 ID_j 为本 RC 的 AN,然后生成报文 $P_i(ID_j, MAC_k(ID_j))$,如图 1 中⑤所示,ID_i 将 P_i 传送给其他新节点,随后删除 K_{ts} 和 BS 坐标,并转入睡眠状态。

⑤ 其他新节点接收 $P_i(ID_j, MAC_k(ID_j))$,验证 ID_j 的合法性,如果合法,接受 ID_j 为本 RC 的 AN,删除 K_v 和 BS 坐标,并转入睡眠状态,结束。

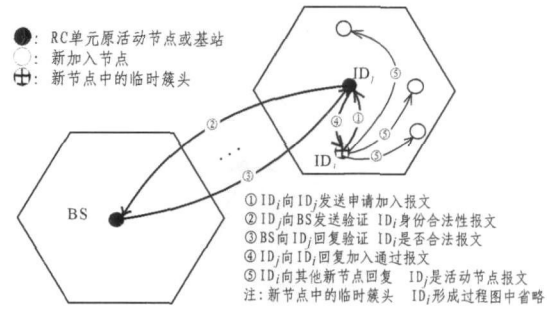

图 1　新节点加入有 AN 的 RC 过程

Fig.1　The Process of New Node Adding to RC with AN

2.2.2　新节点加入无 AN 的 RC

1) RC 内新 AN 的产生

RC 内新 AN 的产生包括 4 个步骤,其中前 3 个步骤的内容与新节点加入有 AN 的 RC 情形的前 3 个步骤内容相同,第四步骤为新 AN 的确认,其内容如下:临时簇头 ID_i 产生报文 $P_i(K_v, ID_{in}, MAC_{i0}(ID_{in}))$,$ID_i$ 将 P_i 广播发送给 ID_i 所在 RC 的 AN。由于该 RC 没有 AN,在规定的时限内没收到应答报文,则 ID_i 认定自己为本 RC 的新 AN。接下来如图 2 中①所示,ID_i 告知本 RC 其他节点其为新 AN,其他新节点收到告知信息后,标记 ID_i 为新 AN,删除 K_{ts} 和 BS 坐标,转入睡眠状态。

2) 新 AN 与其他 RC 内 AN 之间的身份认证。

新 AN 为建立与其他 RC 通信,需与周围 AN 之间确认对方身份的合法性,确认的步骤如下。

① 新活动节点 ID_i 生成要求建立邻居关系的报文 $P_i(K_v, ID_i, MAC_{i0}(ID_i))$,如图 2 中②所示,

ID_i将P_i广播发送给周围RC的AN。

② 设播撒批次为K_j的邻居ID_j收到P_i，若$F^{v-j}(K_v)$值与K_j相同，ID_j确认ID_i为新AN；ID_j生成报文$P_j(ID_j, ID_i, MAC_{j0}(ID_i), MAC_{j0}(ID_j, ID_i, MAC_{j0}(ID_i)))$，如图2中③所示，$ID_j$将$P_j$传递给BS。

③ BS接收报文P_j，验证P_j和ID_i的合法性，如果合法，BS生成报文$P_0(ID_j, MAC_{j0}(ID_j), MAC_{0j}(ID_j, MAC_{j0}(ID_j)))$，如图2中④所示，BS发送报文$P_0$。

④ ID_j接收P_0并验证P_0，如果合法，ID_j确认ID_i为合法邻居节点，接下来如图2中⑤所示，ID_j发送确认报文$P_j(ID_j, MAC_{j0}(ID_j))$给$ID_i$。

⑤ ID_i接收P_j并验证ID_j，如果合法，接受ID_j为邻居AN，删除K_{ts}和BS坐标，结束；如果P_j不合法，丢弃P_j，睡眠一段时间后，继续发送确认报文，直到加入网络或超过规定的安全时限。

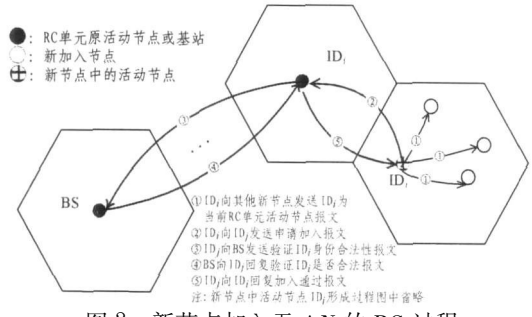

图2 新节点加入无AN的RC过程

Fig.2 Process of New Node Adding to RC without AN

3 ESTCP性能分析

3.1 新节点加入有AN的RC安全性分析

根据单向哈希密钥链特性，攻击者无法通过已有的K_i值伪造K_i后面的K_j值，这样在局部范围内通过新节点中的K_j值可以检测出其身份，有效防止了攻击者伪装成新节点不断要求加入网络的DoS攻击。

虽然上述DoS攻击被防止了，但如图3所示的新节点无法加入网络的情形仍会发生。该情形中攻击者ID_a通过侦听通信链路获得播撒批次K_v和伪造其坐标为RC中最小坐标，使其当选为临时簇头。ID_a当选为临时簇头后，发送要求加入的报文给ID_j，ID_j收到后再发送给BS认证，由于ID_a没有K_s，BS检验出其非法，拒绝其加入，造成以ID_a为临时簇头的其他新节点也无法加入网络。

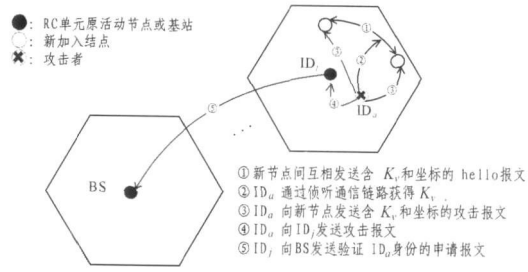

图3 新节点无法加入网络情形.

Fig.3 Case of New Nodes Unable to Add to Network

ESTCP使用临时公共对称密钥技术防止了上述问题。新节点之间通信的报文通过K_{ts}认证，由于攻击者没有K_{ts}，不能通过验证，无法加入到新节点簇中，因此，无法阻止合法新节点加入网络。ESTCP使用该技术还解决了新节点之间的合法身份确认问题，新节点之间通过使用K_{ts}产生ID认证码来相互确认对方的身份。另外，K_{ts}在新节点加入网络后，会被删除，节约了节点的存储空间。

ESTCP中新节点与原AN之间身份的合法性确认通过BS实现。新节点使用K_s生成其ID的认证码，含有认证码的信息经由RC的原AN被发送给BS进行认证，从而防止了攻击者伪造新节点身份进行攻击。

ESTCP还考虑了如何尽量减少认证新节点产生的能耗问题。通常情况下，如果RC内有n个新节点要求加入就会产生n次到BS的认证过程，造成网络能量过多的消耗。为避免每一个新节点加入都与BS进行认证，ESTCP在新节点之间选取临时簇头和原AN通信。携带其他新节点信息的临时簇头通过认证后，再通知簇中其他新节点认证已通过。

3.2 新节点加入无AN的RC安全性分析

对于这种情形的安全性分析与§3.1中情况基本相同，两者新节点加入过程的不同之处在于一种情形是临时簇头与RC内AN之间的认证，另一种情形是临时簇头(即RC内新AN)与邻居RC内AN之间的认证，这两种情形的认证原理类同，其安全性分析也相似，这里不再进行描述。

4 模拟实验

由于ESTCP已增加了安全机制，协议本身具备安全性，现主要仿真分析新加入节点对网络中AN能耗影响。仿真工具采用NS2，实验场景假定随机产生3 000个节点分布在800×800 m^2

场地上的 632 个 RC 中,节点感知半径为 20 m,通信半径为 40 m,采用与文献[10]一样的能量消耗模型。

首先,分析受攻击 AN 的能耗情况。设定网络中只存在一个发起 DoS 攻击的攻击者,攻击者每秒发送 100 个报文。实验结果如图 4 所示。结果表明,当网络中有 DoS 攻击但无防御时,AN 能量被大量消耗;ESTCP 能够对 DoS 攻击作出有效防御,将能量消耗限制到一个相对较低的水平。

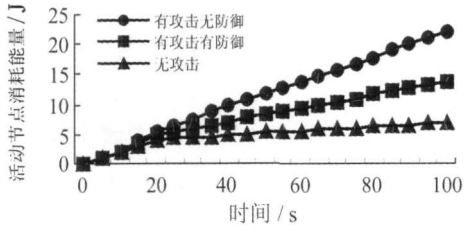

图 4　同情形下活动节点消耗的能量

Fig. 4　Consumption Energy of AN in Diffirent Cases

其次,分析了加入新节点个数对参与新节点认证的相关 AN 平均消耗能量的影响,并比较了新节点先形成临时簇再进行认证和新节点不形成簇直接进行认证这两种情形,即有簇加入和无簇加入情形,实验结果如图 5 所示。结果表明,当仅有一个节点加入 RC 时,无簇加入情形中 AN 平均能耗略低于有簇加入情形中 AN 平均能耗,这是由于有簇新节点之间成簇需要时间,AN 此时处于空闲状态,而处于空闲状态的 AN 同样消耗能量;当有多个节点加入到 RC 中时,无簇加入情形中 AN 平均能耗随着新节点个数的增多越来越多,且变化幅度较大,而有簇加入情形中 AN 平均能耗虽然也是越来越多,但变化幅度很小,这是由于无簇加入情形中每增加一个新节点,就要增加一次到 BS 的认证过程,而有簇加入情形中只需一次到 BS 的认证过程就可实现多个新节点认证。因此,对有多个新节点加入到同一 RC 情形,ESTCP 能够有效地减少网络中 AN 的能量消耗。

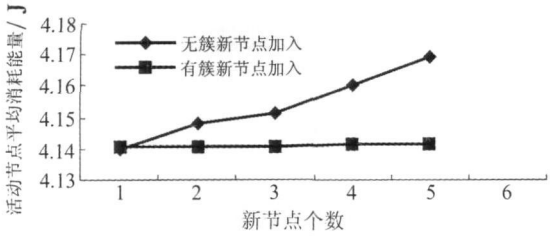

图 5　新节点个数与活动节点平均消耗能量关系

Fig. 5　Relation of Number of New Nodes and AN Average Consumption Energy

参 考 文 献

[1] Younis M, Ghumman K, Eltoweissy M. Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks[J]. IEEE Transactions on Parallel and Distribution System, 2006, 17(8): 865-882

[2] Bekara C, Laurent-Maknavicius M. A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks[C]. The 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), New York, USA, 2007

[3] Wang B T, Schulzrinne H. An IP Traceback Mechanism for Reflective DoS Attacks[C]. Canadian Conference on Electrical and Computer Engineering, Ontario, Canada, 2004

[4] Santi P. Topology control in Wireless ad Hoc and Sensor Networks[J]. ACM Computing Surveys, 2005, 37(2): 164-194

[5] Zhang H, Arora A. GS3: Scalable Self-configuration and Self-healing in Wireless Sensor Networks[J]. Computer Networks (Elsevier), 2003, 43(4): 459-480

[6] Wang X, Berger T. Topology Control, Resources Allocation and Routing in Wireless Sensor Networks[C]. The 12th IEEE MASCOTS, Volendam, Netherlands, 2004

[7] Wang X, Berger T. Self-organizing Redundancy Cellular Architecture for Wireless Sensor Networks[C]. IEEE Wireless Communications and Networking Conference, New Orleans, LA, USA, 2005

[8] Karlof C, Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures[J]. Ad Hoc Networks, 2003(1): 293-315

[9] Yang H, Ye F, Yuan Y, et al. Toward Resilient Security in Wireless Sensor Networks[C]. The ACM MobiHoc 2005, Cologne, Germany, 2005

[10] Heinzelman W B, Chandrakasan A P, Balakrishnan H. An Application-specific Protocol Rrchitecture for Wireless Microsensor Networks[J]. IEEE Transactions on Wireless Communications, 2002, 1(4): 660-670

第一作者简介:王新胜,讲师,博士生。从事无线传感器网络研究。

E-mail:wxs@ujs.edu.cn

(下转第 1050 页)

tection algorithms can not satisfy the unique requirement of grids, an efficient and scalable failure detection algorithm is then presented. According to the characteristics of grids and the small world theory, the authors established a small world based grid system model and a fault detection model; Combined unreliable fault detection method with heartbeat strategy and grey prediction model, they designed a dynamic heartbeat mechanism, and presented the efficient and scalable fault detection algorithm for grid systems further. They also analyzed the performance of the algorithm theoretically, such as how to select performance factors, as well as accuracy, completeness and scalability of the algorithm. At last, experimental result demonstrates that the algorithm is valid and effective, can be used for fault detection under grid environments.

Key words: grid; small-world; grey prediction; heartbeat strategy; fault detection

About the first author: JI Xiaobo, Ph. D candidate, majors in trusted computing and grid computing.
E-mail: bati0716@126.com

(上接第1045页)

Energy-efficient Secure Topology Control Protocol for Wireless Sensor Networks

WANG Xinsheng[1] *ZHAN Yongzhao*[1] *WANG Liangmin*[1,2]
(1 School of Computer Science and Communication Engineering, Jiangsu University, 301 Xuefu Road, Zhenjiang 212013, China)
(2 School of Computer Science and Engineering, Southeast University, 2 Sipailou, Nanjing 210018, China)

Abstract: Saving energy and security are a pair of contradictions demand of application research in wireless sensor networks(WSN). In order to reconcile this pair of contradictions, energy-efficient secure topology control protocol (ESTCP), an energy-efficient secure topology control protocol for wireless sensor networks is presented. In ESTCP, structured topology is formed according to node locations. In order to control new nodes in different situations securely adding to network, techniques of one way hash chain and symmetric cryptographic key are adopted in ESTCP. And temporal clusters are formed among new nodes for reducing energy consumption caused by new nodes authentication. Analysis and simulation results show that ESTCP effectively guarantees the security of topology control in consuming less resource.

Key words: sensor network; topology control; security

About the first author: WANG Xinsheng, lecturer, Ph.D candidate, majors in wireless sensor networks.
E-mail: wxs@ujs.edu.cn