Key management in wireless sensor networks focusing on predistribution by group deployment

Alexander Regler
Betreuerin: Corinna Schmitt
Seminar Innovative Sensorknoten: Betrieb, Netze und Anwendungen SS2010
Lehrstuhl Netzarchitekturen und Netzdienste, Lehrstuhl Betriebssysteme und Systemarchitektur
Fakultät für Informatik, Technische Universität München
Email: regleral@in.tum.de

KURZFASSUNG

Die Sicherheit von Sensornetzen effizient zu gewährleisten, stellt aufgrund der limitierten Speicher- und Leistungsfähigkeit im Vergleich zu anderen Netzwerken eine ungleich komplexere Aufgabe dar. In dieser Arbeit wird ein gruppenbasiertes Verfahren präsentiert, das durch eine Vorinitialisierung der Sensoren sichere Kommunikationsverbindungen ermöglicht. Die Konnektivität, der Grad an Sicherheit und der Speicherbedarf können mittels Parameter flexibel der jeweiligen Anwendung angepasst werden.

Schlüsselworte

Sensornetzwerk, Schlüsselvorverteilung, Gruppenausbringung, Transversal Design

1. EINLEITUNG

Sensornetze erfreuen sich dank ihrer sinkenden Kosten, aber auch aufgrund technischer Fortschritte immer größerer Beliebtheit. Sie bestehen aus mehreren Sensorknoten – Geräten, welche physische Größen, wie Temperatur oder Feuchtigkeit, messen und drahtlos miteinander kommunizieren können [2]. Sensornetze werden mittlerweile in einer Vielzahl von Bereichen eingesetzt, beispielsweise zur Überwachung von Tieren, zum Lokalisieren von Lawinenverschütteten, in der Medizin zur Kontrolle der Lebenszeichen eines Patienten oder im militärischen Bereich zur Verfolgung der eigenen Militärfahrzeuge [1].

Wie in jedem anderen Netzwerk werden auch in Sensornetzwerken geheime und vertrauliche Daten ausgetauscht, die geschützt werden müssen. Allerdings besitzen Sensorknoten je nach Anwendung eine im Vergleich zu gewöhnlichen Netzwerken stark eingeschränkte Energie- und Rechenleistung sowie beschränkte Speicherfähigkeit [3]. Bewährte Verfahren aus der Public-Key-Kryptographie, wie der Diffie-Hellman-Schlüsselaustausch oder eine RSA-Signatur, stellen sehr hohe Anforderungen an die Rechenleistung und den Speicher eines Sensorknotens. Deshalb sollten diese in Sensornetzen ausschließlich bei Applikationen, deren benötigter Sicherheitsgrad diesen zusätzlichen Aufwand unbedingt erforderlich macht, eingesetzt werden.

Eine Alternative zur aufwändigen Public-Key-Kryptographie ist das Verteilen von Schlüsseln auf die Sensorknoten, bevor das Sensornetzwerk aktiv wird. Mit Hilfe der verteilten Schlüssel soll ein Sensorknoten dann eine gesicherte Verbindung zu einem anderen Sensorknoten des aktiven Netzwerkes aufbauen können. Dieses Schema wird im Folgenden als *Schlüsselvorverteilung* (key predistribution) bezeichnet [2]. Eine leicht modifizierte Variante der Schlüsselvorverteilung wird mit Blom's Schema ab Kapitel 4.1 betrachtet. An Stelle der direkten Speicherung der Schlüssel werden hierbei die Sensorknoten mit Polynomen zur Schlüsselgenerierung initialisiert.

Die Ausbringung der Sensorknoten nach der Schlüsselvorverteilung kann hierbei auf unterschiedliche Weise vollzogen werden. Eine Möglichkeit stellt die so genannte *Gruppenausbringung* dar [2]. Diese Ausbringung kann zum Beispiel durch die Benutzung mehrerer Fahrzeuge realisiert werden, bei der jedes Fahrzeug eine Menge von Sensorknoten, eine so genannte *Gruppe*, ausbringt. Sämtliche ausgebrachte Sensorknotengruppen sollen nach der Ausbringung das gemeinsame Sensornetz bilden.

Diese Arbeit konzentriert sich auf ein 2008 von Keith M. Martin, Maura B. Paterson und Douglas R. Stinson entwickeltes Verfahren der Schlüsselvorverteilung, das optimiert ist für eine Ausbringung der Sensorknoten eines Netzwerkes in Gruppen [2]. Hierbei wird gezeigt, dass dieses Verfahren gegenüber anderen vor allem aufgrund seiner Flexibilität Vorteile hinsichtlich der Konnektivität, des Schutzes vor unbefugtem Zugriff und des Speicherbedarfs besitzt.

In Kapitel 2 wird zunächst das Umfeld, in dem das Verfahren von Martin, Paterson und Stinson eingesetzt werden kann, charakterisiert. Anschließend werden in Kapitel 3 Kriterien zur Bewertung von Schlüsselvorverteilungsverfahren eingeführt. Blom's Schema (Kapitel 4.1), das Verfahren von Liu, Ning und Du und dessen Beschränkungen (Kapitel 4.2) sowie die mathematische Grundlage Transversal Design (Kapitel 4.3) dienen dem Verständnis des in Kapitel 4.4 vorgestellten Verfahrens von Martin, Paterson und Stinson. Dieses Verfahren wird hinsichtlich seiner Konnektivität (Kapitel 5.1), seines Schutzes vor unbefugtem Zugriff (Kapitel 5.2) und seiner Anforderungen an die Sensorknoten (Kapitel 5.3) bewertet. Die Ergebnisse werden in Kapitel 6 zusammengefasst.

2. ABGRENZUNG DES UMFELDS

Wie in der Einleitung bereits angesprochen, besitzen Sensorknoten Eigenschaften, die sich direkt auf die Gestaltung eines Verfahrens auswirken [3]:

- beschränkte Rechenleistung
- wenig Speicherplatz
- begrenzte Energieressource

- eingeschränkte Kommunikationsweite
- geringe Bandbreite der Kommunikation.

Daher wird eine Schlüsselvorverteilung für die Sensorknoten vorgenommen, d.h. jeder Sensorknoten wird mit bestimmten Schlüsseln initialisiert [2]. Die Knoten besitzen noch keinen Kontakt zueinander. Jedoch steht bereits bei der Schlüsselvorverteilung fest, dass sich die Sensorknoten in Gruppen gleicher Größe befinden werden und in welchen Gruppen die Knoten ausgebracht werden. Somit ist im Vorfeld für jedes beliebige Paar von Sensorknoten bekannt, ob sie sich in derselben Gruppe befinden werden oder nicht. Dementsprechend werden Schlüssel auf die Sensorknoten verteilt.

Anschließend werden die Sensorknoten in den festgelegten Gruppen ausgebracht. Hierbei werden sowohl die Gruppen als auch die Sensorknoten innerhalb einer Gruppe zufällig verteilt, d.h. es ist nicht bekannt, an welchem Ort sich die einzelnen Sensorknoten nach der Verteilung befinden werden.

Die Gruppenausbringung hat hierbei gegenüber einer zufälligen Ausbringung eines jeden einzelnen Sensorknotens den entscheidenden Vorteil, dass die Konnektivität des Sensornetzes durch die partielle Ortsgebundenheit der einzelnen ausgebrachten Gruppen erhöht werden kann.

Bei den Gruppen des Sensornetzes unterscheidet man grundsätzlich zwei Gestaltungsalternativen [2]:

- heterogene Gruppen
- homogene Gruppen.

Heterogene Gruppen bestehen aus mindestens einem Sensorknoten, der eine bessere technische Ausstattung im Vergleich zu den restlichen Sensorknoten aufweist und z.B. Kommunikationsaufgaben zwischen Gruppen übernimmt. Dahingegen wird eine homogene Gruppe aus einer Menge gleichartiger Sensorknoten gebildet.

Das in dieser Arbeit vorgestellte Verfahren geht von homogenen Sensorgruppen aus.

3. GÜTEKRITERIEN EINES VERFAHRENS

Zur Bewertung von Verfahren müssen Kriterien festgelegt werden.

Eine wesentliche Rolle bei der Bewertung eines Verfahrens zur Schlüsselvorverteilung spielen drei Aspekte, die Konnektivität des Sensornetzes, der Speicheraufwand eines jeden Sensorknotens und die Sicherheit des Sensornetzes vor einer unbefugten Übernahme.

3.1 Konnektivität

Nach der Ausbringung der Sensorknoten versuchen diese, gemeinsame Verbindungen herzustellen, so dass jeder Sensorknoten mit jedem beliebigen Knoten (auch über andere Knoten) kommunizieren kann.

Eine *direkte Verbindung* zwischen zwei Sensorknoten wird genau dann aufgebaut, wenn beide Knoten den gleichen Schlüssel besitzen und der Abstand der beiden Knoten kleiner oder gleich der drahtlosen Kommunikationsreichweite ist [2].

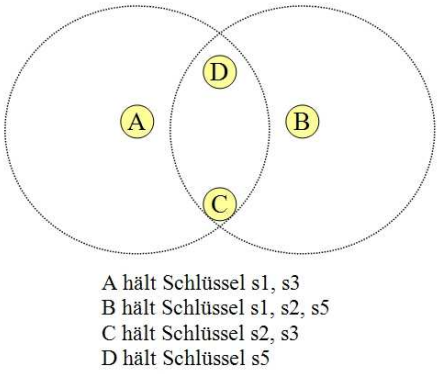

Abbildung 1: Sensornetz der Sensorknoten A, B, C und D nach der Initialisierung und Ausbringung

Zum Beispiel halten die Sensorknoten A und B des Sensornetzes in Abbildung 1 mit *s1* denselben Schlüssel, können aber keine direkte Verbindung aufbauen, da B nicht innerhalb des Kommunikationsradius von A liegt und umgekehrt. Stattdessen können {A,C}, {B,C} und {B,D} eine gemeinsame Verbindung, wie in Abbildung 2 dargestellt, aufbauen, wenn man davon ausgeht, dass die aufgrund der Übersichtlichkeit nicht eingezeichneten Kommunikationsradien von C und D denen von A und B entsprechen.

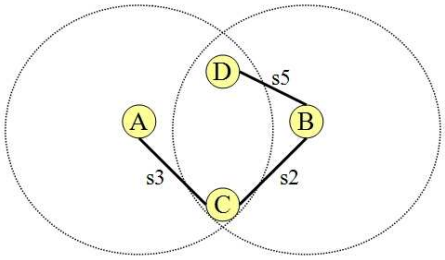

Abbildung 2: Sensornetz der Sensorknoten A, B, C und D nach dem Aufbau der Verbindungen

Das Ziel des Verbindungsaufbaus ist es, dass ein zusammenhängender Graph entsteht, damit je zwei Sensorknoten innerhalb des Netzwerkes miteinander kommunizieren können und somit eine optimale *globale Konnektivität* (global connectivity) entsteht [7]. Kann kein zusammenhängender Graph gebildet werden, so ist mindestens ein Sensorknoten vom Sensornetz abgeschnitten. Je mehr Sensorknoten vom Sensornetz getrennt sind, desto geringer ist die globale Konnektivität.

Die *lokale Konnektivität* (local connectivity) hingegen ist definiert als die Wahrscheinlichkeit, dass lokal benachbarte Knoten miteinander sicher und effizient kommunizieren können [7]. Sie ist als Bewertungskriterium im Vergleich zur globalen Konnektivität besser geeignet, da von den Abhängigkeiten bei der physischen Gruppenausbringung abstrahiert wird und zudem eine hohe lokale Konnektivität auch ein Indiz für eine hohe globale Konnektivität ist [2].

Zur Messung und Bewertung der lokalen Konnektivität werden die so genannten *2-Hop-Wege* (2-hop pathes) eingeführt [2]. Dies sind Kommunikationspfade zwischen zwei Knoten X und Y, die mit maximal einem weiteren Knoten Z gebildet werden können, wobei Z entweder Mitglied der Gruppe von X oder von Y ist. 2-Hop-Wege umfassen somit exakt die direkte Verbindung

zwischen X und Y sowie Verbindungen über einen Knoten Z, der nicht zu einer dritten Gruppe gehört.

Angenommen, die Knoten A, B, C und D in Abbildung 2 bilden eine Gruppe. Dann besteht zwischen A und B über den Knoten C genau ein 2-Hop-Weg. Zwischen A und D besteht kein 2-Hop-Weg.

3.2 Sicherheit vor unbefugtem Zugriff

Es wird davon ausgegangen, dass einzelne Sensorknoten von Unbefugten übernommen und ausgelesen werden können. Diese erhalten somit die Schlüssel, mit denen der ausgelesene Sensorknoten kommuniziert hat. Alle weiteren Verbindungen, die diesen Schlüssel nutzen, werden dadurch unsicher.

In den folgenden Abschnitten sei *fail(s)* die Wahrscheinlichkeit, dass eine sichere Verbindung zwischen zwei noch nicht übernommenen Knoten unsicher wird, nachdem Unbefugte Zugriff auf *s* zufällige Knoten erlangt haben [2]. Je kleiner *fail(s)*, desto größer ist die Sicherheit vor einer unbefugten Übernahme.

3.3 Speicheraufwand

Ein Verfahren muss so konstruiert sein, dass es möglichst wenig Speicherplatz auf den Sensorknoten belegt, da Sensorknoten in der Regel nur eine geringe Speicherkapazität zur Verfügung stellen und diese auch von anderen Aufgaben in Anspruch genommen wird [2].

Angenommen, „unterschiedliche paarweise Schlüssel“ (distinct pairwise keys) wird als Schlüsselvorverteilungsverfahren verwendet, d.h. jedem Paar von Sensorknoten wird je ein Schlüssel zur Kommunikation zugewiesen und keine zwei Paare von Sensorknoten besitzen den gleichen Schlüssel [2]. Dann muss jeder Sensorknoten in einem Sensornetz bestehend aus n Knoten $n-1$ Schlüssel speichern. Dies bedeutet bei größeren Sensornetzen einen sehr hohen Speicheraufwand, wohingegen die Konnektivität und die Sicherheit vor einem unbefugten Zugriff optimal sind.

Der Speicheraufwand ist hingegen minimal, wenn zum Beispiel ein Sensornetz lediglich einen Schlüssel besitzt und jeder Sensorknoten genau diesen Schlüssel hält. Ebenso ist die Konnektivität optimal, jedoch bietet dies nur eine minimale Sicherheit vor einem unbefugten Zugriff. Ist ein Sensorknoten übernommen, so ist das gesamte Sensornetz unsicher.

4. VERFAHREN ZUR SCHLÜSSELVORVERTEILUNG

4.1 Blom’s Schema

1984 entwickelte Rolf Blom ein symmetrisches Schlüsselgenerierungssystem (symmetric key generation system). Dieses wird in dem nachfolgend vorgestellten, flexiblen Schlüsselvorverteilungsverfahren von Martin, Paterson und Stinson verwendet, um in einer Menge von Sensorknoten eine gesicherte direkte Verbindung zwischen jedem Paar von Sensorknoten herstellen zu können. Die für diese Arbeit relevanten Grundzüge des Schemas werden im Folgenden erklärt, für weitere Details sei auf [5] verwiesen.

4.1.1 *Verfahren*

Blom’s Schema verwendet ein symmetrisches, zweidimensionales Polynom $P(x,y)$ über einem endlichen Feld $GF(q)$, d.h. $P(i,j) = P(j,i)$ für alle $i,j \in GF(q)$ [2]. Jeder Sensorknoten mit einer ID i wird mit einem so genannten *Anteil* (share) von P, einem eindimensionalem Polynom $h_i(y)$ vom Grad t, initialisiert. Hierbei wird der Anteil $h_i(y)$ aus dem Polynom P berechnet, es gilt: $h_i(y) = P(i,y)$ für eine ID i. Damit eine Verbindung zwischen zwei Sensorknoten mit IDs i und j aufgebaut werden kann, muss der gemeinsame Schlüssel $K_{ij} = h_i(j) = h_j(i)$ von jedem Sensorknoten aus seinem zugeordneten Anteil berechnet werden. Somit kann zwischen jedem Paar von Sensorknoten eine sichere Verbindung aufgebaut werden.

4.1.2 *Eigenschaften*

Dieses Schema besitzt aufgrund je eines verwendeten Schlüssels bei der Kommunikation zwischen je zwei Sensorknoten dieselbe Konnektivität im Vergleich zu dem in Kapitel 3.3 erwähnten Verfahren „unterschiedliche paarweise Schlüssel“.

Im Speicher eines jeden Sensorknotens werden genau $t+1$ Koeffizienten eines Polynoms vom Grad t, dem Anteil, gespeichert, um eine Verbindung zu allen anderen n Sensorknoten des Sensornetzes herstellen zu können.

Ein unbefugter Zugriff des Sensornetzes ist erst dann möglich, wenn $t+1$ oder mehr Sensorknoten des Netzes übernommen wurden, denn dann kann das Polynom P interpoliert und somit alle Schlüssel berechnet werden.

4.2 Liu, Ning und Du’s Verfahren

Liu, Ning und Du haben 2005 ein Verfahren zur Schlüsselvorverteilung unter Verwendung von Gruppenausbringung veröffentlicht [4], welches einen Ausgangspunkt für das von Martin, Paterson und Stinson entwickelte Verfahren darstellt und zu dessen Verständnis beiträgt. Es wird im Folgenden zunächst kurz vorgestellt, bevor anschließend aufgezeigt wird, unter welchen Bedingungen dessen Einsatz an Grenzen stößt.

4.2.1 *Verfahren*

In Liu, Ning und Du’s Verfahren werden die Sensorknoten auf Gruppen verteilt. Zudem werden zur Kommunikation zwischen den Gruppen so genannte *Kreuzgruppen* (cross-groups) gebildet. Hierbei enthält jede Kreuzgruppe genau einen Knoten aus jeder Gruppe und jeder Sensorknoten einer gewöhnlichen Gruppe ist in genau einer Kreuzgruppe enthalten.

Innerhalb einer Gruppe oder Kreuzgruppe soll jeder Knoten mit jedem anderen Knoten der gleichen Gruppe über jeweils einen gemeinsamen Schlüssel der Kommunikationspartner kommunizieren können. Hierzu werden Schlüssel innerhalb der Gruppen nach dem Prinzip der „unterschiedlichen paarweisen Schlüsseln“ (siehe Kapitel 3.3) oder nach Blom’s Schema (siehe Kapitel 4.1) vergeben. Somit kann durch die festgelegten Gruppen und Kreuzgruppen sowie einer entsprechenden Schlüsselvorverteilung ein zusammenhängendes Sensornetz nach der Sensorenausbringung gebildet werden.

Im Folgenden wird dieses Verfahren an einem Beispiel gezeigt. Eine Menge von 9 Sensorknoten a bis i soll in Gruppen zu je drei Knoten aufgeteilt werden. Abbildung 3 zeigt eine mögliche Verteilung. Hierbei wurden die Gruppen {a,b,c}, {d,e,f} und {g,h,i} gewählt. Drei mögliche Kreuzgruppen, die Liu, Ning und Du’s Schema genügen, sind {a,d,g}, {b,e,h} und {c,f,i}. Nun kann beispielsweise Knoten a mit Knoten b, c, d und g direkt kommunizieren, sofern die physischen Gegebenheiten dazu erfüllt werden.

Abbildung 3 veranschaulicht das resultierende Sensornetz graphisch. Eine gewöhnliche Gruppe ist durch ein Oval dargestellt, eine Kreuzgruppe entsteht durch je zwei Verbindungen zwischen 3 Knoten.

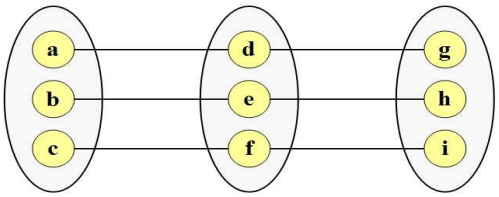

Abbildung 3: Beispiel zu Liu, Ning und Du's Verfahren

4.2.2 *Beschränkungen*

Hinsichtlich der in Kapitel 3 vorgestellten Gütekriterien wird im Folgenden gezeigt, dass das von Liu, Ning und Du entwickelte Verfahren im Bereich der Konnektivität Schwächen aufweist.

Zunächst lässt sich aber feststellen, dass bei einer Schlüsselvorverteilung innerhalb der Gruppen und Kreuzgruppen unter Verwendung von Blom's Schema eine individuelle Abstimmung zwischen Speicheraufwand der einzelnen Sensorknoten und der Sicherheit vor einem unbefugten Zugriff getroffen werden kann [2]. Je größer der Grad t gewählt wird, desto geschützter ist das Sensornetz vor einer unbefugten Übernahme. Je kleiner der Grad t gewählt wird, desto geringer ist der Speicherbedarf der einzelnen Sensorknoten.

Die Konnektivität dieses Verfahrens weist allerdings Mängel auf [2].

Angenommen, es werden n Sensorknoten in λ Gruppen ausgebracht, dann beträgt die Wahrscheinlichkeit, dass sich Knoten verschiedener Gruppen auch innerhalb einer Kreuzgruppe befinden und miteinander kommunizieren können, λ / n .

Bei einer Ausbringung in wenigen Gruppen, also bei einem kleinen Wert von λ, ist diese Wahrscheinlichkeit sehr gering. Dies birgt einerseits das Risiko, dass ganze Gruppen nicht mit dem Sensornetz verbunden werden können und andererseits kann es zu Engpässen zwischen zwei Gruppen kommen, zwischen denen nur wenige Sensorknoten für die Verbindung zuständig sind.

Das in Kapitel 4.4 vorgestellte Verfahren zur Schlüsselvorverteilung mit Transversal Designs löst diese Beschränkung der Konnektivität. Hierzu wird ein zusätzlicher Parameter eingeführt, wodurch die Konnektivität zwischen Gruppen auch bei einer Ausbringung in wenigen Gruppen beliebig verändert werden kann.

4.3 Transversal Design

Bevor das Verfahren von Martin, Paterson und Stinson erläutert wird, wird zu dessen Verständnis zunächst mit einem Transversal Design eine dazu benötigte mathematische Grundlage eingeführt.

Definition 1 [2]: Ein *Transversal Design TD(k, n)* besteht aus

- einer Menge V mit genau $k \bullet n$ Elementen. Die Elemente werden als *Punkte* bezeichnet.
- einer Partition G der Punkte von V in k Mengen mit je n Elementen. Die Elemente von G werden als *Design-Gruppen* bezeichnet.
- und einer Menge B, bestehend aus k-Teilmengen von V mit der Eigenschaft, dass jedes Paar unterschiedlicher Punkte in genau einem Element von G ∪ B enthalten ist. Die Elemente von B werden als *Blöcke* bezeichnet.

Beispielsweise sei k = 2 und n = 3. Dann besitzt die Menge V des Transversal Designs TD(2,3) 6 Elemente. Diese Elemente seien mit A bis F bezeichnet:

$$V = \{A,B,C,D,E,F\}$$

Die Menge V lässt sich unter anderem wie folgt in Elemente der Menge G zerlegen:

Design-Gruppe 1: {A,B,C}

Design-Gruppe 2: {D,E,F}

Eine Menge, bestehend aus allen 2er-Teilmengen der Menge V, enthält $\binom{k \bullet n}{2} = \binom{2 \bullet 3}{2} = 15$ Elemente. Mit der Eigenschaft, dass jedes Paar unterschiedlicher Punkte nur in genau einem Element von G ∪ B enthalten ist, ergibt sich B wie folgt:

$$B = \{\{A,D\},\{A,E\},\{A,F\},$$
$$\{B,D\},\{B,E\},\{B,F\},$$
$$\{C,D\},\{C,E\},\{C,F\}\}$$

Definition 2 [2]: Ein Transversal Design TD(k, n) ist *auflösbar*, falls die Blöcke der Menge B in Mengen B_1, B_2, …, B_S partitioniert werden können, so dass jeder Punkt der Menge V in genau einem Block in jeder dieser Mengen vorkommt. Diese Mengen werden als *Parallelklassen* bezeichnet.

Zur Erläuterung dieser Definition wird das obige Beispiel aufgegriffen. Die dort ermittelte Menge B kann in folgende drei parallele Klassen partitioniert werden:

Parallelklasse 1 = {{A,D},{B,E},{C,F}}

Parallelklasse 2 = {{A,E},{B,F},{C,D}}

Parallelklasse 3 = {{A,F},{B,D},{C,E}}

Die durch ein auflösbares Transversal Design erhaltenen Parallelklassen werden im Verfahren von Martin, Paterson und Stinson benötigt.

4.4 Schlüsselvorverteilung mit einem Transversal Design

Im Folgenden wird das von Keith M. Martin, Maura B. Paterson und Douglas R. Stinson entwickelte Verfahren vorgestellt [2]. Die Definition bezieht sich auf ein Sensornetz mit n^2 Sensorknoten, welche in λ Gruppen G_1, G_2, …, G_λ der Größe n^2 / λ ausgebracht werden sollen.

Definition 3: Gegeben sei eine Primzahlpotenz n und zwei positive Zahlen k und t, für die gilt: $1 \le k \le n$, $\lambda \mid n$ (λ ist ein Teiler von n) und $0 \le t < (n^2 / \lambda) - 1$.

1. Zerlege die n Parallelklassen P_1, P_2, …, P_n des Transversal Designs TD(k, n) in λ Mengen mit je n / λ Parallelklassen. Diese Mengen werden im Folgenden als S_1, S_2 bis S_λ bezeichnet und jede Menge S_i enthält genau n^2 / λ Blöcke.

2. Ordne jedem Block einen Sensorknoten zu. Alle zu den Blöcken einer Menge S_i zugeordneten Sensorknoten bilden die Gruppe G_i.
3. Jedem Punkt der Menge V des TD(k, n) wird ein Polynom von Blom's Schema zugeordnet und jedem Sensorknoten, dessen Block den entsprechenden Punkt aus V enthält, wird ein Anteil vom Grad t zugeordnet.
4. Jeder Parallelklasse P_i wird ein Polynom gemäß Blom's Schema zugeordnet und jedem Sensorknoten, dessen Block in der Parallelklasse P_i liegt, wird ein Anteil vom Grad t zugeordnet.

Durch Anwendung dieser Definition können alle n^2 Sensorknoten mit Anteilen nach Blom's Schema initialisiert werden.

Als erläuterndes Beispiel sei $k = 2$, $n = 3$, $\lambda = 3$ und $t = 1$. Dann wird das in Definition 3 beschriebene Verfahren ausgeführt:

1. Die im vorangegangenen Kapitel 4.3 ermittelten drei Parallelklassen zu einem auflösbaren TD(2,3) können wegen $k = 2$ und $n = 3$ wieder aufgegriffen werden. Da $\lambda = n$ sind dies die Mengen S_1, S_2 und S_3.
2. Nun werden den Blöcken aus S_i die Sensorknoten a bis i zugeordnet und es entstehen folgende Gruppen:

$$G_1 = \{a,b,c\}$$
$$G_2 = \{d,e,f\}$$
$$G_3 = \{g,h,i\}$$

3. Sei $f_x(X)$ die Notation für den Anteil nach Blom's Schema, der dem Sensorknoten x, dessen zugeordneter Block den Punkt X enthält, zugeordnet ist. Sensorknoten a wurde dem Block {A,D} zugeordnet und somit bekommt a die Anteile $f_a(A)$ sowie $f_a(D)$. Analoges gilt für die weiteren Sensorknoten. Somit wurden Anteile zur Kommunikation zwischen den Gruppen G_1, G_2 und G_3 verteilt und implizit Kreuzgruppen gebildet.
4. Sei $f_x(i)$ die Notation für den Anteil nach Blom's Schema, der dem Sensorknoten x, dessen zugeordneter Block in der i-ten Parallelklasse P_i liegt, zugeordnet ist. Der Sensorknoten a liegt in der Parallelklasse 1 und somit bekommt a den Anteil $f_a(1)$. Analoges gilt für die weiteren Sensorknoten. Durch die verteilten Anteile kann eine sichere Kommunikation innerhalb einer Gruppe stattfinden.

Damit ist das Verfahren vollständig ausgeführt. Die Sensorknoten benötigen keine weiteren Informationen zum sicheren Kommunikationsaufbau innerhalb des Sensornetzes. Es ergibt sich die folgende Verteilung der Anteile auf die Sensorknoten:

a: $\{f_a(A), f_a(D), f_a(1)\}$ d: $\{f_d(A), f_d(E), f_d(2)\}$

b: $\{f_b(B), f_b(E), f_b(1)\}$ e: $\{f_e(B), f_e(F), f_e(2)\}$

c: $\{f_c(C), f_c(F), f_c(1)\}$ f: $\{f_f(C), f_f(D), f_f(2)\}$

g: $\{f_g(A), f_g(F), f_g(3)\}$

h: $\{f_h(B), f_h(D), f_h(3)\}$

i: $\{f_i(C), f_i(E), f_i(3)\}$

Nun können die Sensorknoten, physische Gegebenheiten vorausgesetzt, entsprechend ihrer gehaltenen Anteile miteinander direkte Verbindungen aufbauen. Sensorknoten a kann mit den Sensorknoten b und c über die Anteile $f_x(1)$ kommunizieren, mit den Sensorknoten d und g über $f_x(A)$ und mit den Sensorknoten f und h über $f_x(D)$. D.h. Sensorknoten a kann innerhalb der Gruppe {a,b,c} sowie den Kreuzgruppen {a,d,g} und {a,f,h} mit allen anderen Knoten der Gruppen direkt kommunizieren. Analoges gilt für alle weiteren Sensorknoten.

Eine graphische Veranschaulichung der Gruppen, innerhalb derer direkte Kommunikation zwischen jedem beliebigen Knotenpaar stattfinden kann, findet sich in Abbildung 4. Hierbei wird eine Kreuzgruppe jeweils durch zwei gestrichelte (bzw. durchgezogene) Verbindungen zwischen drei Knoten dargestellt, eine gewöhnliche Gruppe durch ein umschließendes Oval. Insgesamt werden somit die entstandenen sechs Kreuzgruppen und die drei gewöhnlichen Gruppen des Beispiels repräsentiert.

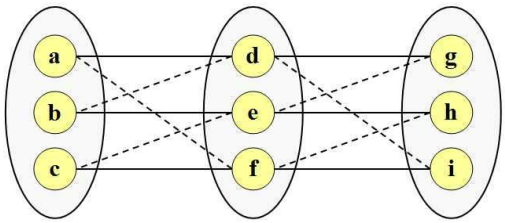

Abbildung 4: Beispiel zur Schlüsselvorverteilung mit einem Transversal Design

5. BEWERTUNG DES VERFAHRENS

5.1 Konnektivität

5.1.1 *Flexibilität der Konnektivität*

Die Konnektivität des vorgestellten Schlüsselvorverteilungsverfahrens mit einem Transversal Design kann flexibel in Abhängigkeit der Parameter k und λ eingestellt werden [2]. Dies ist ein Vorteil gegenüber dem Verfahren von Liu, Ning und Du, da dieses keine Parameter zur Einstellung einer gewünschten Konnektivität bietet. In dem Verfahren mit einem Transversal Design hingegen bewirkt eine Erhöhung von k oder λ stets eine Konnektivitätssteigerung.

Allerdings hat diese Konnektivitätssteigerung auch ihre Grenzen. Für eine Erhöhung von k wird mehr Speicherplatz auf jedem Sensorknoten benötigt. Eine Erhöhung von λ, und somit eine Erhöhung der Gruppenanzahl, kann bei einer sehr hohen Anzahl der Gruppen zu Schwierigkeiten in der praktischen Umsetzung führen.

5.1.2 *Vergleich mit anderen Verfahren mittels Simulationen*

Im Folgenden werden Simulationsumgebungen eingerichtet und durchgeführt [2]. Hierbei wird gezeigt, dass das Verfahren von Martin, Paterson und Stinson (MPS) im Vergleich zu dem Verfahren von Liu, Ning und Du (LND) und einem der bekanntesten zur Schlüsselvorverteilung genutzten Verfahren, das von Eschenauer und Gligor (EG) (für Details siehe [6]), auch bei einem vordefinierten Speicherplatz Vorteile bezüglich der lokalen und globalen Konnektivität bietet.

Die Simulationsumgebung besteht aus einem Sensornetz mit 16384 Sensorknoten, welche in $\lambda = 16$ Gruppen zu je 1024 Knoten ausgebracht werden. In jedem Sensorknoten können $m = 32$ Schlüssel bzw. Koeffizienten gespeichert werden. Zudem wird mit Pr_1 der erwartete Anteil der Knotenpaare, die eine Verbindung mit einem gemeinsamen Schlüssel aufbauen können, bei jeder Simulationsdurchführung vorab festgelegt. Diese Bindungen

ermöglichen insgesamt einen gerechten Vergleich zwischen den einzelnen Verfahren.

Der Speicherplatz der Verfahren LND und MPS wird durch feste Parameterwerte für *k* und *t* fixiert. Das ohne Gruppenausbringung realisierte Verfahren EG wird durch den Parameter *K* beschränkt, der die Anzahl aller verwendeter Schlüssel repräsentiert.

Anhand des festgelegten Umfelds können die die lokale Konnektivität beschreibenden Größen $2Hop_g$ und $2Hop_k$ berechnet werden. $2Hop_g$ (bzw. $2Hop_k$) entspricht der Wahrscheinlichkeit, dass zwei Knoten einer Gruppe (bzw. einer Kreuzgruppe) eine gemeinsame Verbindung über einen 2-Hop-Weg aufbauen können.

Außerdem wird mit *E(K)* eine die globale Konnektivität beschreibende Größe ermittelt, welche die durchschnittliche Anzahl an Sensorknoten der größten zusammenhängenden Komponente in dem entstandenen Sensornetzwerk, basierend auf 100 Wegen, abschätzt. Hierbei wird eine Ausbringung der Knoten auf ein Gebiet von 500 m x 500 m simuliert, wobei alle Knoten einer Gruppe gleichmäßig in einem Kreis mit Radius 100 m verteilt werden und jeder Knoten eine Kommunikationsreichweite von 6 m besitzt.

Die Simulationsergebnisse finden sich in Tabelle 1.

Tabelle 1: Konnektivitätsmessung eines Sensornetzes bestehend aus 16 Gruppen mit je 1024 Knoten [2]

Schema	Parameter	Pr_1	$2Hop_g$	$2Hop_k$	E(K)
LND	t = 17	0,0634	1,00	0,0145	1510
MPS	k = 7, t = 3	0,0620	0,329	0,172	2140
EG	K = 15760	0,0630	0,0888	0,114	1800
MPS	k = 15, t = 1	0,124	0,466	0,395	8640
EG	K = 7750	0,124	0,215	0,296	7600
MPS	k = 31, t = 0	0,248	0,713	0,769	13200
EG	K = 3620	0,248	0,518	0,691	12600

Aus der Tabelle ist ersichtlich, dass das Schlüsselvorverteilungsverfahren mit einem Transversal Design (MPS) in jeder Simulation stets eine höhere lokale und globale Konnektivität als das Verfahren EG aufweist – repräsentiert durch die Werte $2Hop_g$, $2Hop_k$ und *E(K)*.

Außerdem zeigt sich in der ersten durchgeführten Simulationsumgebung ein deutlicher Unterschied der globalen Konnektivität zwischen LND und MPS. Hierbei weist die Gruppenausbringung nach LND sogar im Vergleich zur zufälligen Ausbringung nach EG eine schlechtere globale Konnektivität auf (aufgrund der geringen lokalen Konnektivität zwischen den einzelnen Gruppen, ausgedrückt durch $2Hop_k$), so dass von einer Anwendung des LND-Verfahrens in dieser Simulationsumgebung abzuraten ist. Dagegen erzielt das Verfahren MPS aufgrund seiner Flexibilität die besten Simulationsergebnisse.

5.2 Sicherheitskriterien

Sichere Verbindungen zwischen einzelnen Sensorknoten in dem Sensornetz werden mittels Schlüsseln gebildet. Besitzt ein Unbefugter den Verbindungsschlüssel zwischen zwei Sensorknoten, so ist die Verbindung unsicher.

5.2.1 *Sicherheit gegen unbefugten Zugriff*

Ein Maß für die Sicherheit gegen unbefugten Zugriff wurde in Kapitel 3.2. mit *fail(s)* eingeführt, wobei *s* die Anzahl der durch Unbefugte übernommenen Knoten darstellt. Für das zur Schlüsselvergabe verwendete Schema von Blom gilt, dass eine gesicherte Verbindung zwischen zwei Knoten genau dann unsicher wird, wenn mehr als *t* Knoten mit einem entsprechenden Anteil übernommen wurden. Deshalb gilt für das Verfahren der Schlüsselvorverteilung mit einem Transversal Design [2]:

$$fail(s) = \begin{cases} 0 & \text{für} \quad s \le t \\ 1 - \sum_{i=0}^{t} \frac{\binom{n-2}{i}\binom{n^2-n}{s-i}}{\binom{n^2-2}{s}} & \text{für} \quad s > t \end{cases}$$

Die Sicherheit von Blom's Schema und damit die Sicherheit des Verfahrens von Martin, Paterson und Stinson kann flexibel, aber zu Lasten des Speicherbedarfs, erhöht werden, indem Polynome höheren Grades verwendet werden. D.h. je größer *t* gewählt wird, desto sicherer ist das Verfahren.

5.2.2 *Vergleich mit anderen Verfahren mittels Simulationen*

Im Folgenden wird gezeigt, dass das Verfahren von Martin, Paterson und Stinson (MPS) auch bezüglich der Sicherheit vor einem unbefugten Zugriff im Vergleich zu dem Verfahren von Liu, Ning und Du (LND) und dem Verfahren von Eschenauer und Gligor (EG) Vorteile besitzt [2].

Betrachtet wird ein Sensornetz mit 16384 Knoten, das durch das Transversal Design TD(39,128) gebildet wurde und aus 16 Gruppen zu je 1024 Knoten besteht. Zur Vergleichbarkeit der Verfahren werden wie in Kapitel 5.1.2 die Parameter *m* und Pr_1 verwendet. Ebenso werden für die Verfahren LND und EG die Formeln für *fail(s)* nach [2] aufgestellt.

Nun können die drei Verfahren in Abhängigkeit der Werte m und Pr_1 miteinander verglichen werden.

Sei $m = 32$ und $Pr_1 \approx 0{,}063$. Die zugehörigen Funktionsverläufe der Funktion *fail(s)* zu den drei Verfahren sind für $s \in [0{,}1000]$ in Abbildung 5 dargestellt.

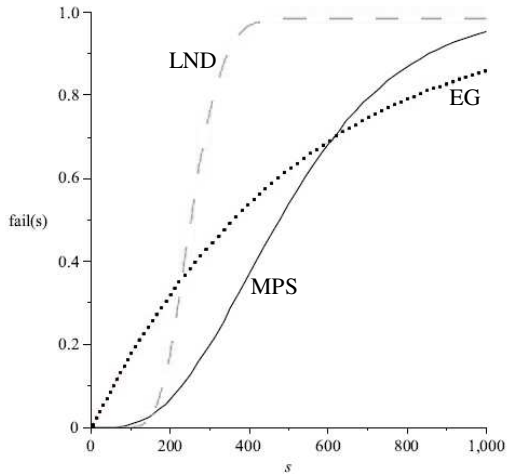

Abbildung 5: Vergleich des Verfahrens MPS mit den Verfahren LND und EG für $m = 32$ und $Pr_1 \approx 0{,}063$ [2]

Hierbei erkennt man, dass LND für kleine Werte von s die größte Sicherheit vor einem unbefugten Zugriff bietet, aber bereits ab ca. 300 übernommenen Knoten ist das gesamte Sensornetz unsicher. Dahingegen liefert MPS für Werte von s von ca. 200 bis ca. 600 den besten Widerstand. Erst ab $s \approx 600$ ist das Verfahren von Eschenauer und Grigor am günstigsten, allerdings erweist es sich bis $s \approx 600$ als deutlich schlechter im Vergleich zu MPS. Das Verfahren von Martin, Paterson und Stinson weist somit im Vergleich zu LND und EG für $Pr_1 \approx 0{,}063$ günstige Sicherheitswerte auf.

5.3 Anforderungen an die Knoten

Das Verfahren stellt hinsichtlich Speicherbedarf und Rechenleistung Anforderungen an einen Sensorknoten.

Auf einem Sensorknoten müssen bei Anwendung des Verfahrens $(k+1)(t+1)$ Schlüssel bzw. Koeffizienten der Polynome von Blom's Schema gespeichert werden und eine dementsprechende Speicherkapazität ist auf jedem Sensorknoten erforderlich [2].

Der Speicherbedarf kann aber durch die beiden Parameter k und t angepasst werden. Je kleiner k oder t, desto weniger Speicherplatz wird auf dem Sensorknoten benötigt. Allerdings bedeutet ein kleinerer Wert für k nach [2] auch Konnektivitätseinbußen und ein geringerer Wert für t eine reduzierte Sicherheit vor unbefugter Übernahme.

Hinsichtlich der Rechenleistung erfordert die Verwendung von Blom's Schema zusätzlichen Rechenaufwand im Vergleich zu herkömmlichen Schlüsselvorverteilungsverfahren, in denen der Schlüssel direkt auf dem Sensorknoten gespeichert wird. Ein zur Kommunikation mit einem anderen Sensorknoten benötigter Schlüssel muss erst berechnet werden, indem das gespeicherte Polynom (der Anteil nach Blom's Schema) mit der Kennung des Kommunikationspartners ausgewertet wird. Dies muss bei jedem Verbindungsaufbau durchgeführt werden.

6. ZUSAMMENFASSUNG

Das vorgestellte Verfahren von Martin, Paterson und Stinson zur Schlüsselvorverteilung bietet zahlreiche Vorteile, es weist aber auch Nachteile gegenüber bewährten Verfahren auf.

Zur Initialisierung der Sensorknoten müssen zunächst mehrere mathematische Schritte und Operationen durchgeführt werden. Andere Verfahren zur Schlüsselvorverteilung, wie beispielsweise das Verfahren von Liu, Ning und Du oder das Verfahren von Eschenauer und Gligor, besitzen einen niedrigeren Komplexitätsgrad und damit eine einfachere Sensorknoteninitialisierung.

Zudem verwendet das Verfahren von Martin, Paterson und Stinson zur Schlüsselgenerierung Blom's Schema. Hierdurch muss ein Sensorknoten bei jedem Aufbau einer sicheren Verbindung zu einem anderen Sensorknoten den gemeinsamen Schlüssel aus seinem gespeichertem Polynom berechnen. Dies wäre bei einer direkten Speicherung der Schlüssel auf den Sensorknoten nicht notwendig.

Dennoch kann trotz der genannten Nachteile der Einsatz des Verfahrens äußerst sinnvoll sein.

Durchgeführte Simulationen demonstrieren, dass das Verfahren von Martin, Paterson und Stinson gegenüber dem Verfahren von Liu, Ning und Du sowie dem Verfahren von Eschenauer und Gligor in bestimmten Umgebungen die besten Ergebnisse hinsichtlich Konnektivität und Sicherheit liefert.

Außerdem kann die Konnektivität und der Schutz vor unbefugtem Zugriff durch zusätzliche Speicherbenutzung mittels Parametereinstellungen gesteigert und somit gezielt, der Anwendung entsprechend, angepasst werden.

Daneben führt auch die Ausweitung der Gruppenanzahl bei der Ausbringung der Sensorknoten zu Konnektivitätssteigerungen.

Insgesamt sollte man aufgrund der dargelegten Verbesserungen und der flexiblen Anpassungsmöglichkeiten den Einsatz dieses Verfahrens in Erwägung ziehen.

Zur Vereinfachung des Verfahrens sowie zur Reduzierung der Rechenoperationen der Sensorknoten könnte anstelle von Blom's Schema ein anderes Verfahren, zum Beispiel das von Eschenauer und Gligor, verwendet werden. Es ist aber fraglich, wie sich dies auf die Konnektivität und die Sicherheit des entstehenden Sensornetzes auswirkt.

7. LITERATURQUELLEN

[1] Römer, K., and Mattern, F. 2004. The design space of wireless sensor networks. IEEE Wireless Communications, Vol. 11, No. 6, pp. 54-61.

[2] Martin, K. M., Paterson, M. B., and Stinson, D. R. 2008. Key predistribution for homogeneous wireless sensor networks with group deployment of nodes. Cryptology ePrint Archive, Report 2008/412.

[3] Chan, H., Perrig, A., and Song, D. 2003. Random key predistribution schemes for sensor networks. SP '03: Proceedings of the 2003 IEEE symposium on security and privacy.

[4] Liu, D., Ning, P., and Du, W., 2008. Group-based key predistribution in wireless sensor networks. ACM transactions on sensor networks, Vol. 4, No. 2, pp. 1-30. DOI = 1340771.1340777

[5] Blom, R., 1985. An optimal class of symmetric key generation systems. Proceedings of the EUROCRYPT 84 workshop on advances in cryptology: theory and application of cryptographic techniques, pp. 335-338.

[6] Eschenauer, L., and Gligor, V. D. 2002. A key management scheme for distributed sensor networks. Proceedings of the 9th ACM conference on computer and communication security, pp. 41-47. DOI = 586110.586117

[7] Lee, J., and Stinson, D. R. 2008. On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. ACM Transactions on Information and System Security, Vol. 11, Issue 2, pp. 1-35. DOI = 1330332.1330333